FORTINET

TechWorkshop Oktober 2018

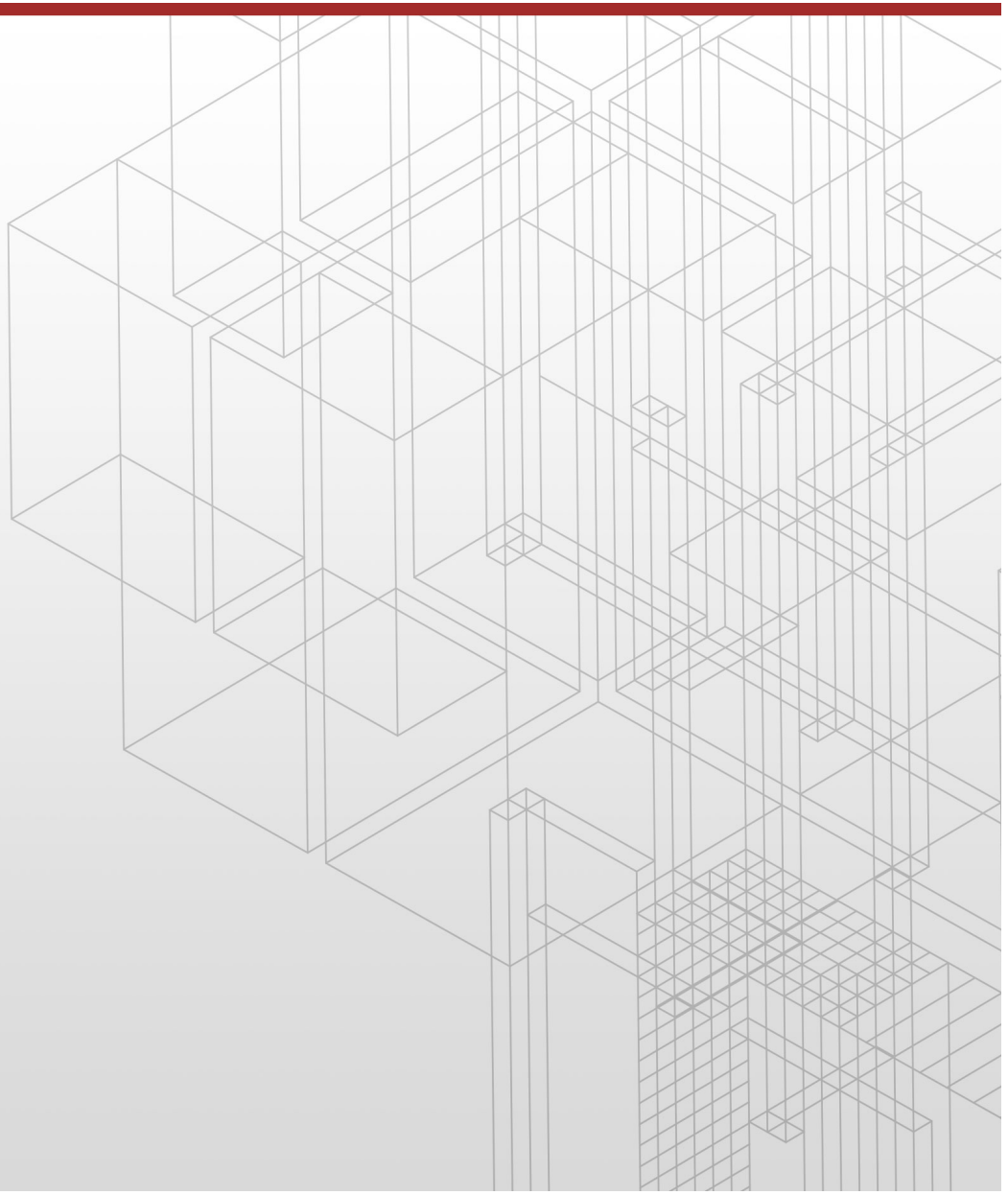
Secure SD-WAN

Markus Frey, Fortinet Systems Engineer

Agenda

- SD-WAN Introduction
- SD-WAN Use Cases
- 3rd Party Verification / Competitive
- FortiOS SD-WAN
- FortiManager SD-WAN

SD-What ?

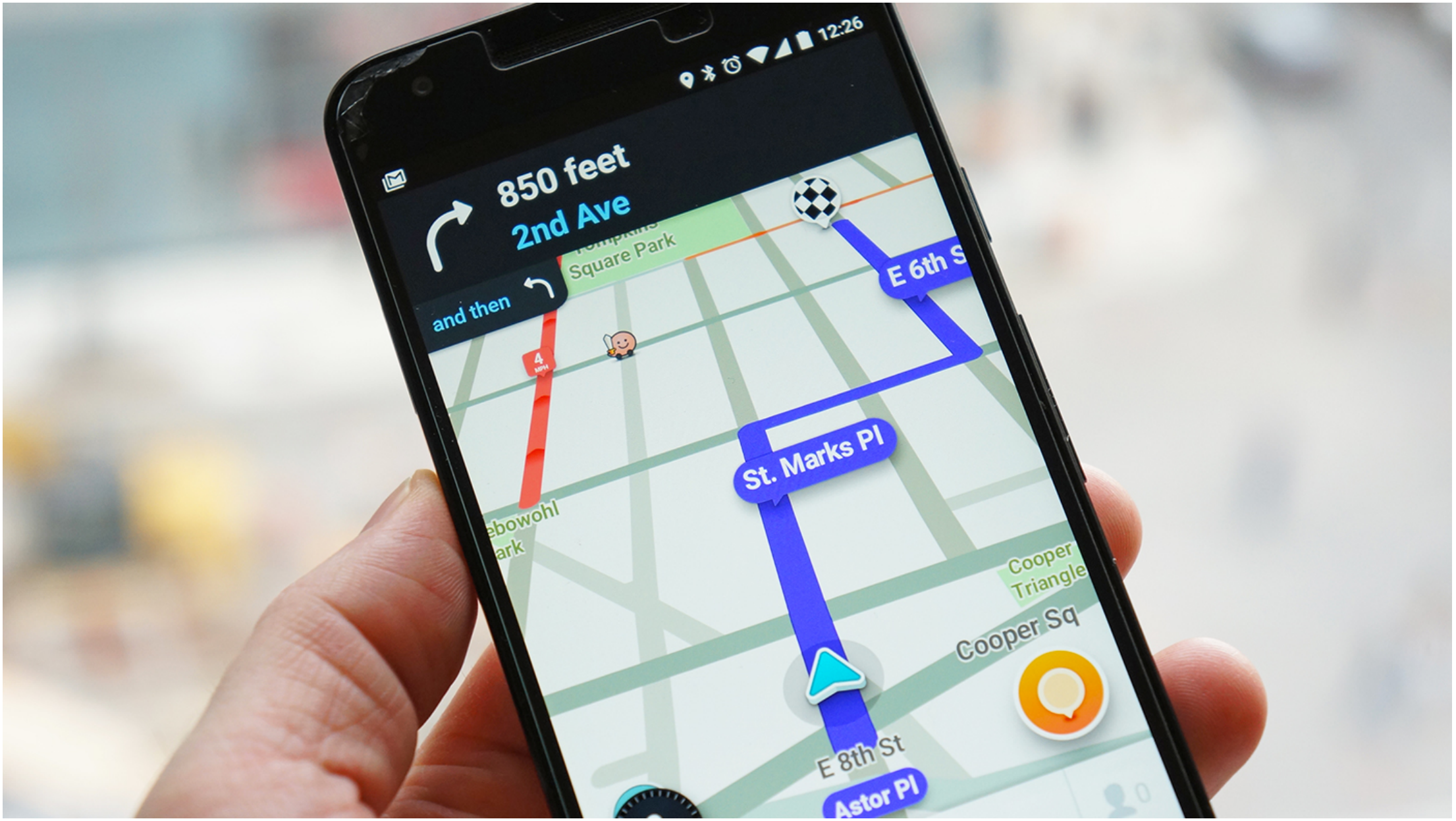


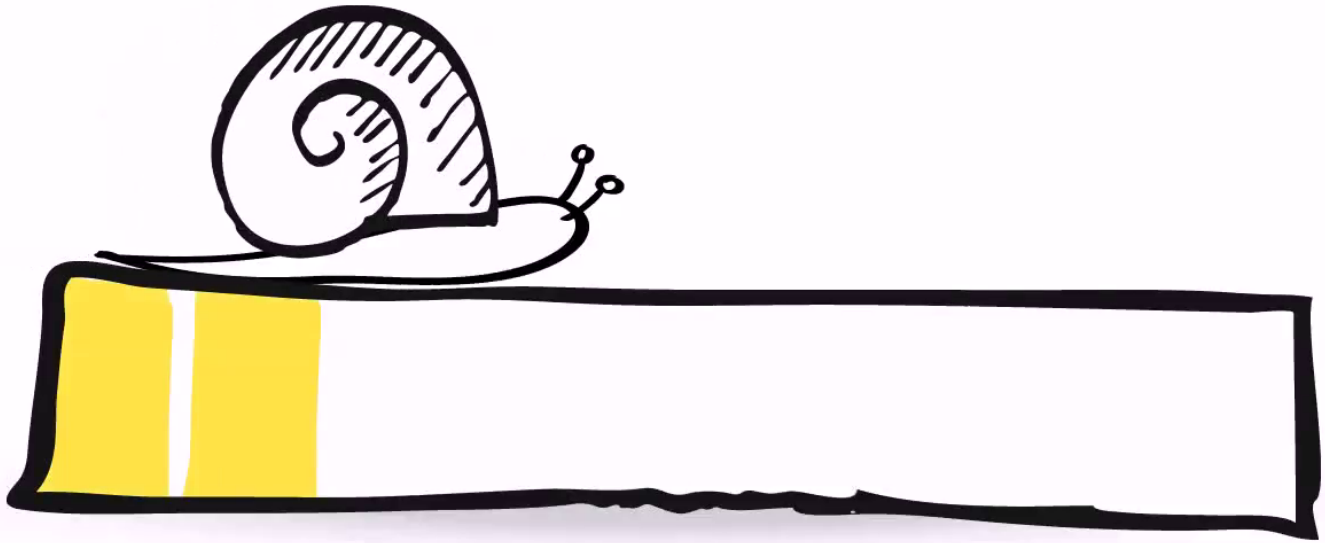
FORTINET

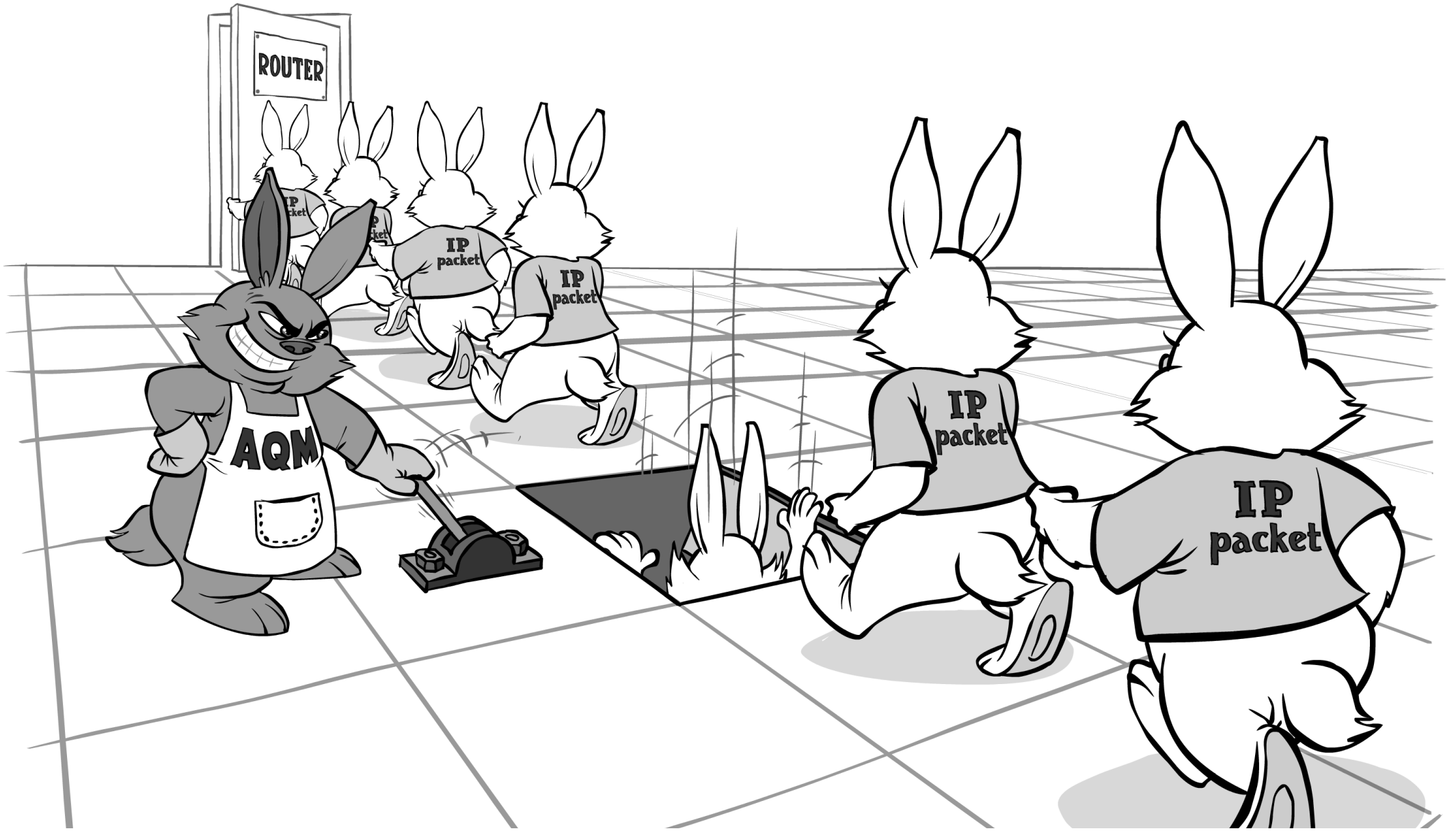

STOP

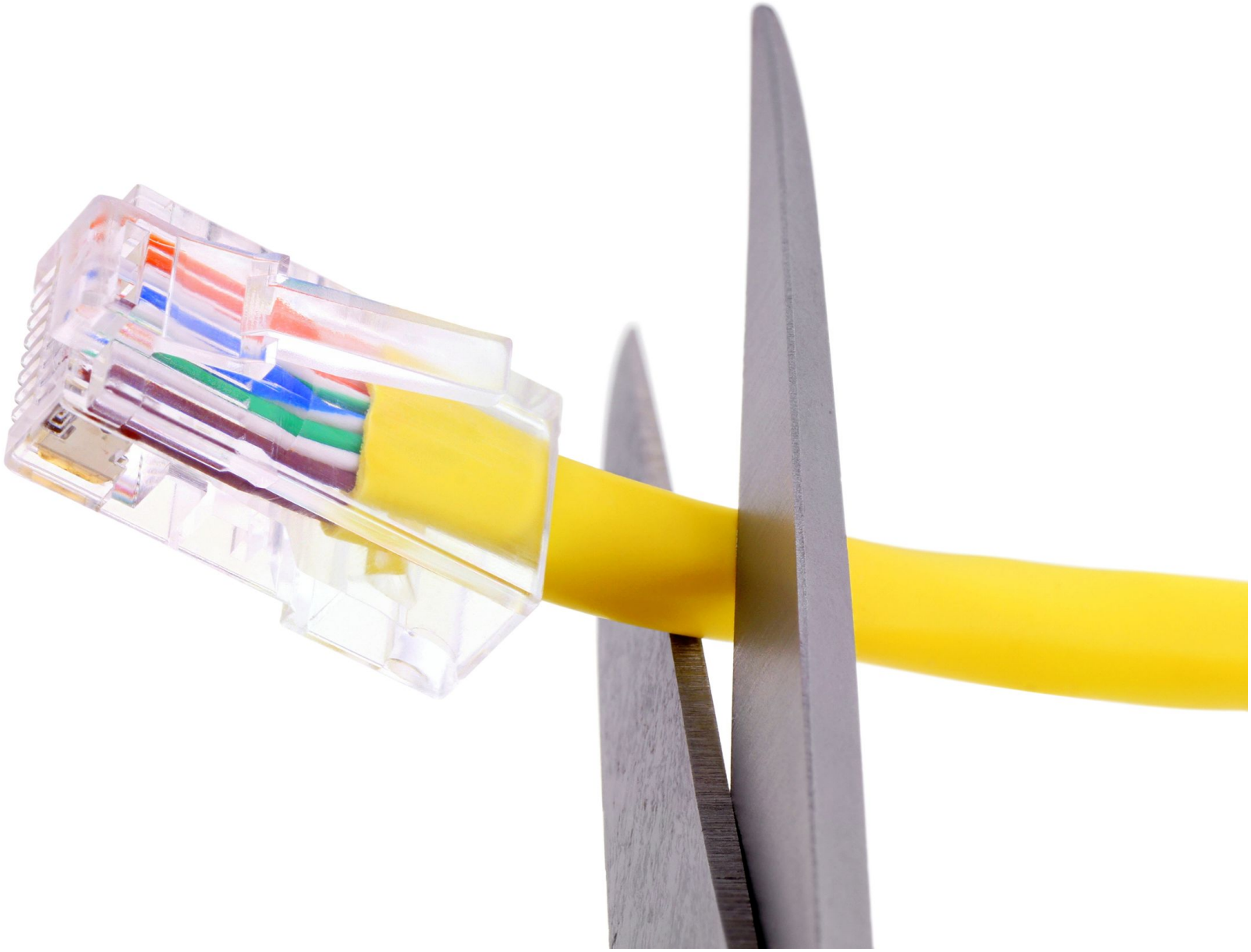

Slow
Down
High
Crash
Rate


HÚNAFLÓI
BREIÐAFJÖRÐUR
FAXAFLÓI
Hofsjökull
Dyngjujökull
Brúarjökull
Langjökull
Mýrdals Jökull
THE MEANING OF ICELANDIC PLACE NAMES
ÜBERSETZUNG ISLÄNDISCHER ORTSNAMEN
SIGNIFICATION DES TOPONYMES ISLANDAIS
ÍSLAND
1:500 000
roadtrip ICELAND
Iceland Road Map
www.icelandroadtrip.com
info@icelandroadtrip.com
HERIDUNORD
PARTIE SEPTENTRIONALE
PARTIE OCCIDENTALE
PARTIE MERIDIONALE


12:26
850 feet
2nd Ave
and then
Square Park
E 6th S
St. Marks Pl
Cooper
Triangle
Cooper Sq
E 8th St
Astor Pl




ROUTER
AQM
IP packet
IP packet
IP packet
IP packet
IP packet



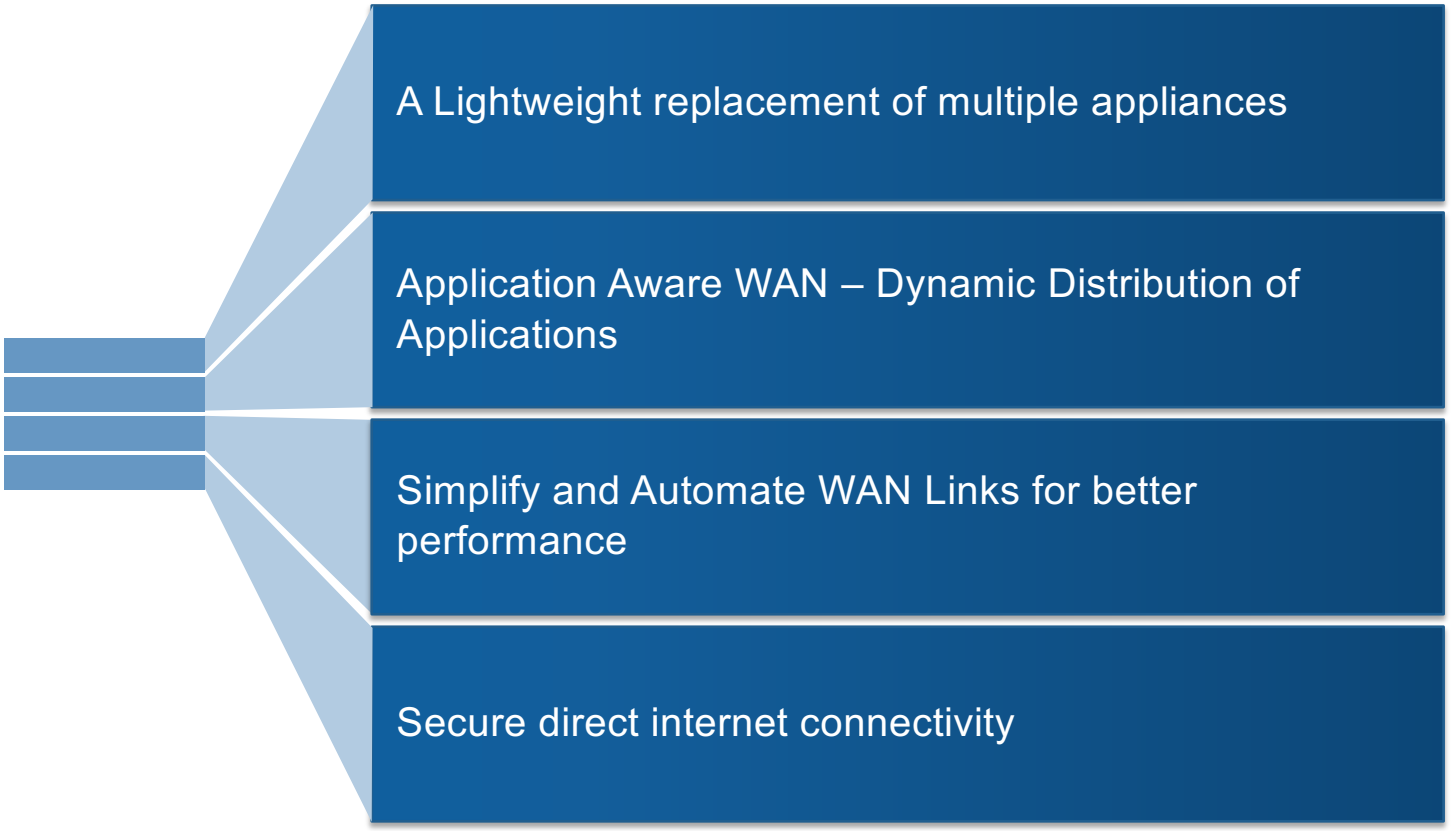

SD-WAN!

SD-WAN Introduction

FORTINET

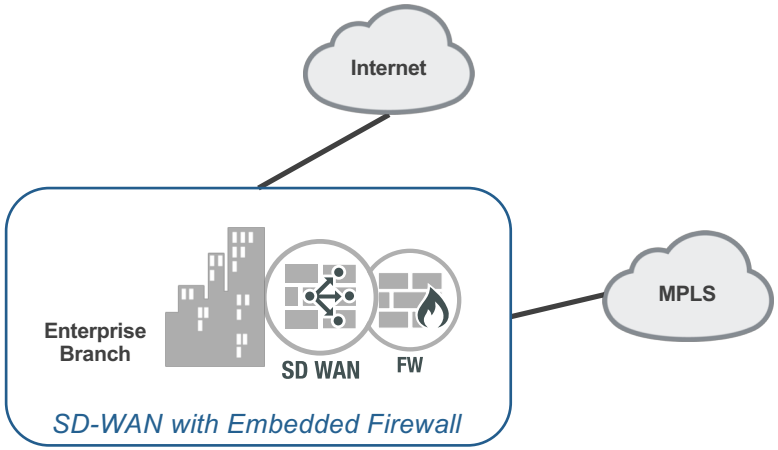
SD-WAN Enables Branch Evolution

Gartner

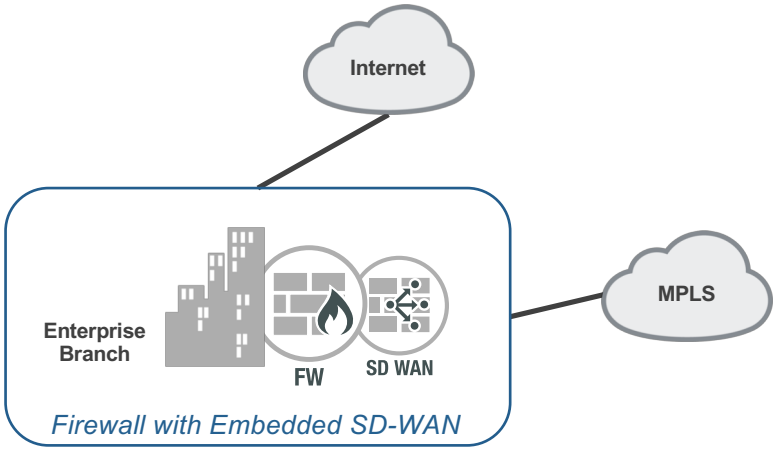


Source: Gartner MG

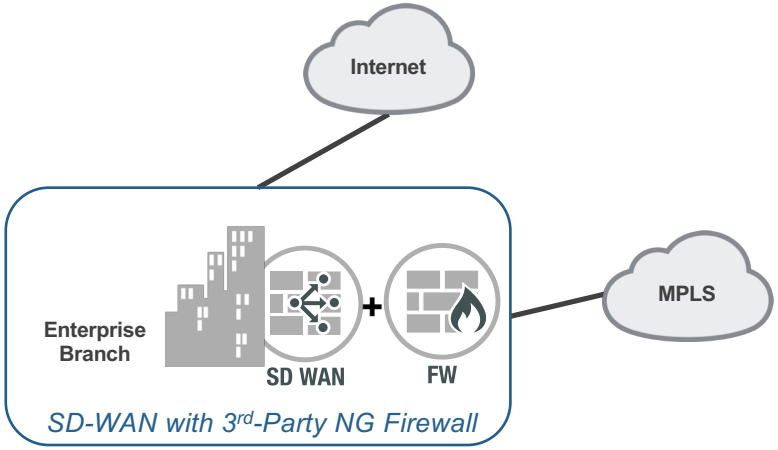
Four architectures to secure SD-WAN by Gartner



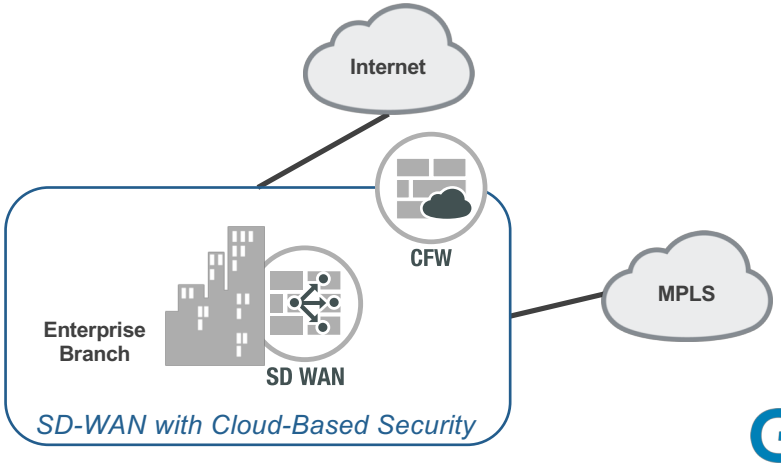
SD-WAN with Embedded Firewall



Firewall with Embedded SD-WAN



SD-WAN with 3rd-Party NG Firewall



SD-WAN with Cloud-Based Security

Gartner

Four architectures to secure SD-WAN by Gartner

	SD-WAN With Embedded Firewall	Firewall With Embedded SD-WAN	SD-WAN With SWG	SD-WAN With Third-Party Firewall
SD-WAN				
Security Level				
Branch Office Types	Smaller branch office with noncritical activities	Larger branch offices with more critical activities	Smaller remote branch office with noncritical activities	Larger branch offices with more critical activities
Relative Cost				
Sample Vendors	Citrix, CloudGenix, Silver Peak, VeloCloud	Barracuda Networks, Cisco Meraki, Fortinet	Symantec, Zscaler	Check Point, Cisco, Fortinet, Juniper Networks, Palo Alto Networks

Full Harvey ball: most; empty Harvey ball: least.

Source: Gartner (October 2017)

Tradicional MPLS vs SDWAN - Comparative

	MPLS	SD WAN
Link Estimated Cost	**10Mb – $700/month**	**3x 30Mbps (3 ISP Providers) 90Mbps – $100,00/month**
Average delivery time	45 days	3 days
Performance	Medium	High
Resilience	Low	High
Tools/Reporting	SNMP, ICMP	Netflow Based, Orchestrators, Solution Controllers, Advanced Application Reporting
Difficulty to install	BGP, OSPF, BFD, QoS (CBWFQ, PQ) Architecture... And convergence does not always work! (Complex Routing, Asymmetry) No tools for application traffic analysis	ZTD, Probes, Visibility, SLA, Alarm, Graphs, GUI, Easy convergence

What Today's Customers are looking for

- **I need to turn up locations quickly**
  - » Temporary pop-up retail locations
  - » Time to provision Leased Lines / MPLS too high
  - » Reduce the on-prem footprint (power, space)
  - » Global supply chain
- **I need scalability and resilience in the move to the cloud**
  - » Prioritize my business critical apps in the cloud (local breakout)
  - » Back up for my MPLS (IPSec Overlay)
  - » Use cheaper, high-bandwidth public internet circuits
  - » Maintain same User Experience
- **Whatever the solution, it needs to be easy to manage**
  - » Zero touch provisioning
  - » Central management

Security?

Forecasts

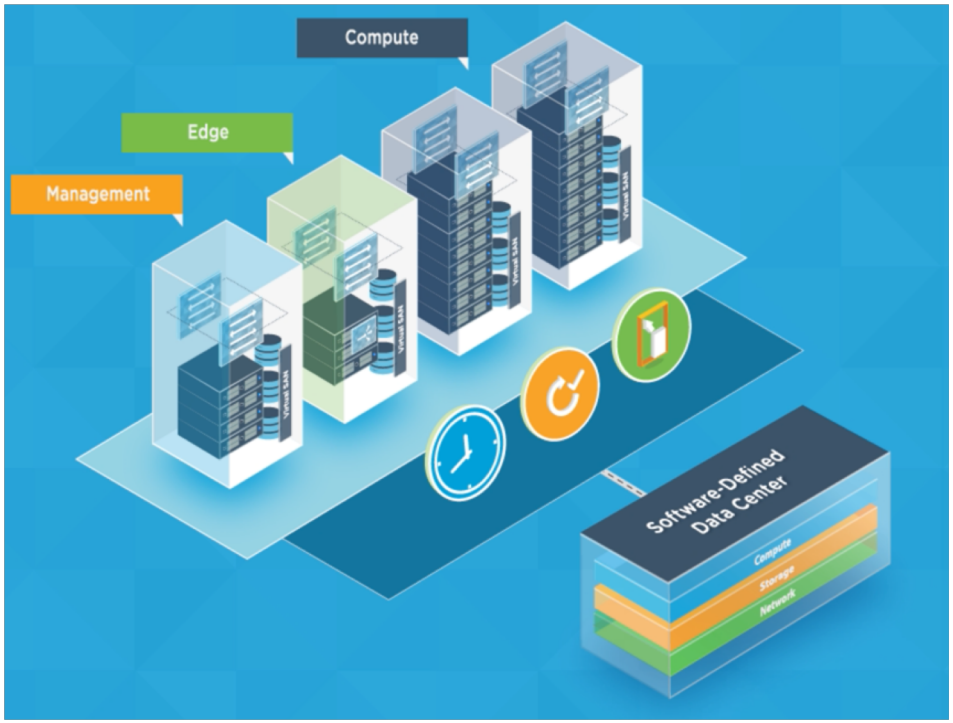
27 JUL 2017

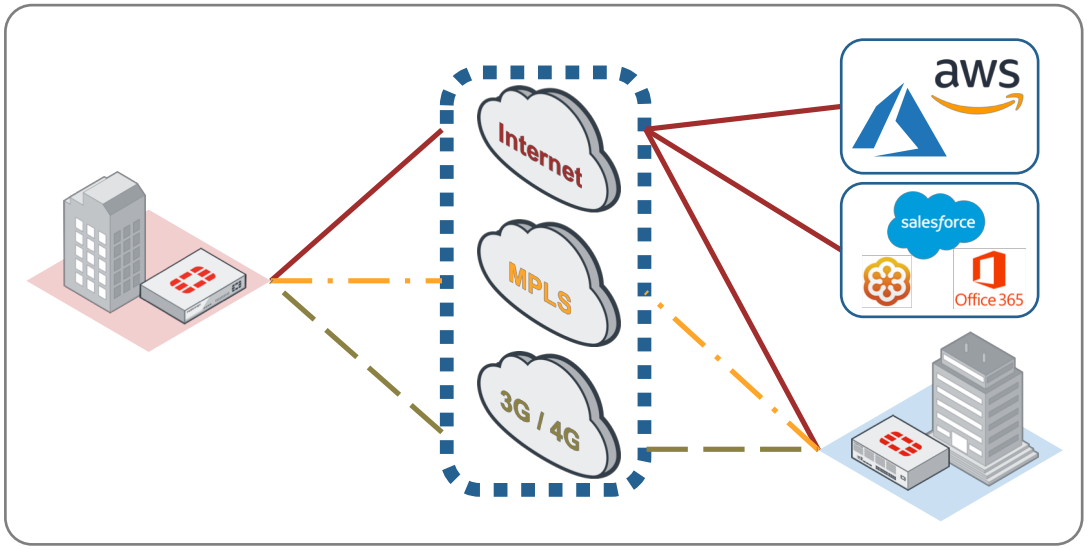
IDC Forecasts SD-WAN Market to Reach $8 Billion in 2021 As Enterprise Branch Network Requirements Accelerate

The **benefits of SD-WAN** include **cost-effective** delivery of business applications, meeting the evolving operational requirements of the modern branch/remote site, **optimizing software-as-a-service** (SaaS) and **cloud-based services** such as UC&C, and improving branch-IT efficiency through **automation**. These benefits have resonated across the spectrum of enterprise IT and service providers alike, ensuring a broad-based uptake for this **new paradigm in WAN architectures**.

https://www.idc.com/getdoc.jsp?containerId=prUS42925117

SDN vs SD-WAN


Compute
Edge
Management
Software-Defined
Data Center


Internet
MPLS
3G / 4G
aws
salesforce
Office 365

Enterprise Branch Going Through Evolution

Today's Enterprise Branch WAN traffic is back-hauled to data-center which degrades SaaS Applications Performance

DX Transformation

62

Average number of cloud applications shows rapid growth of SaaS and IaaS[3]

Inefficient Traditional WAN

70%

Of customers mentioned existing WAN is brittle, slow, expensive and not effective for cloud adoption[2] due to back-haul

Security is "MUST"

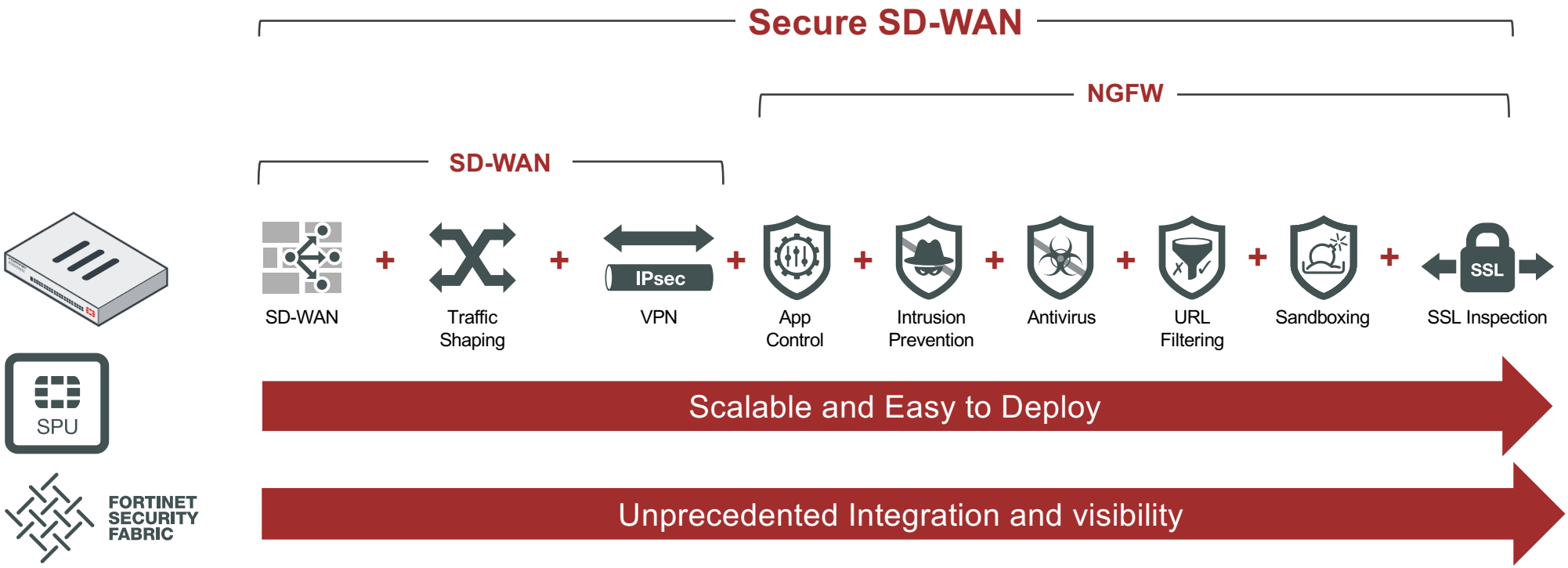
90%

Of SD-WAN vendors do no provide security. With direct internet access, security becomes critical at every branch

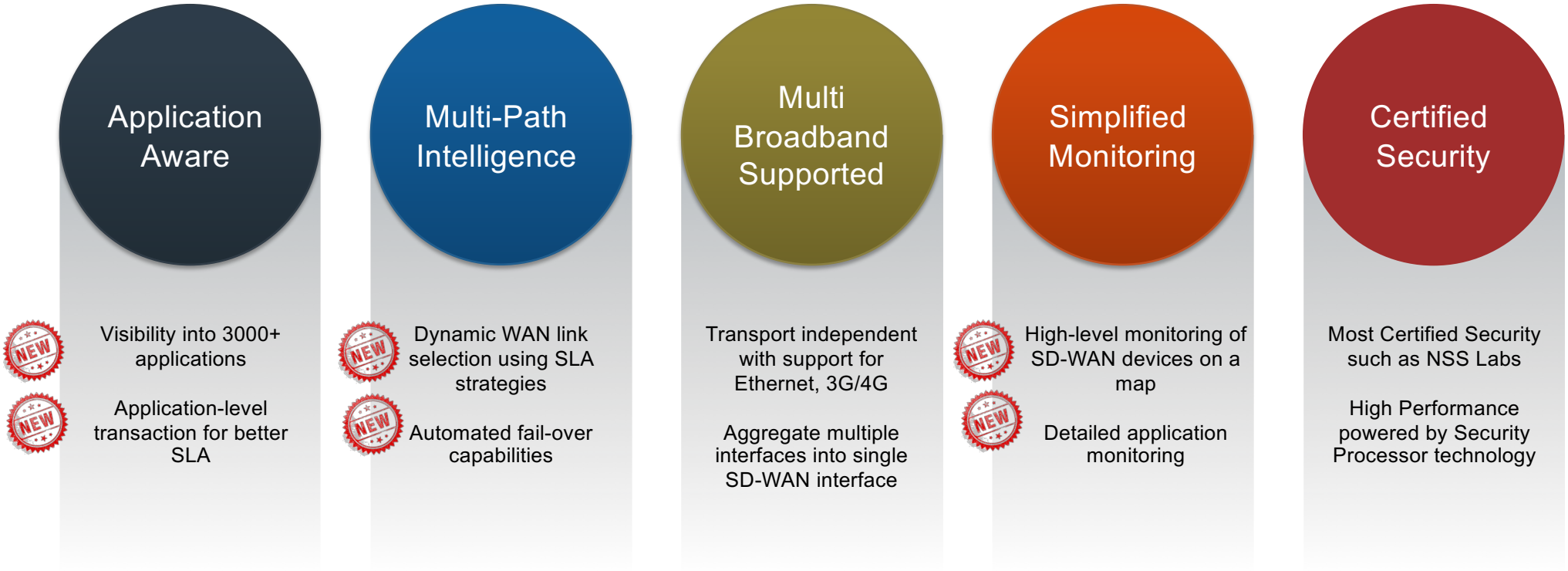
FortiGate Next Generation Firewalls with Integrated SD-WAN

SD-WAN requires direct internet access which requires better security at every branch

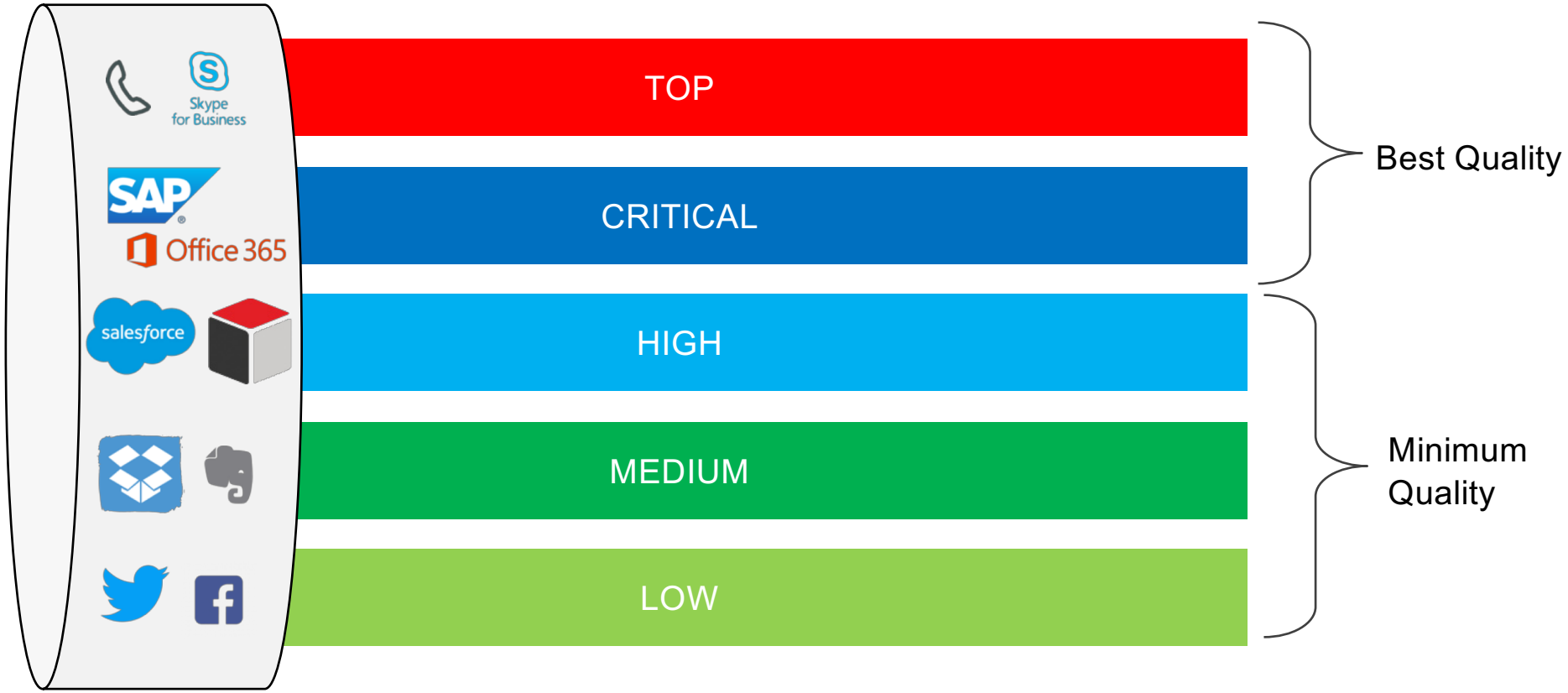
90% of the SD-WAN vendors only offer stateful firewalls which is not enough



FOS 6.0 - Enable Best of Breed SD-WAN



Control Application Performance using Strategized SLA



Performance SLA (For high priority applications)

Application-Level Transaction → **Multiple Measurement Techniques** → **Failover Parameters**

Office 365

Skype for Business

Latency < 200ms

Latency < 100ms
AND
Packet Loss < 1%
AND
Jitter < 30ms

- ❑ Ping
- ❑ HTTP
- ❑ TCP Echo
- ❑ UDP Echo
- ❑ TWAMP

Check Interval

Failure before inactive

Success before restore

Gartner Recognize Fortinet Secure SD-WAN

Gartner®

"Fortinet has a strong and focused SD-WAN Strategy"
10th December 2017

"Fortinet has enhanced their firewalls and integrated advanced SD-WAN requirements "
6th October 2017

- By year-end 2018, more than **50%** of WAN edge infrastructure **refresh initiatives** will be based on **SD-WAN** software/appliances versus traditional routers (up from **less than 5% today**)
- SD-WAN products now incorporate internet perimeter security, but more than **90% of SD-WAN vendors are not** traditional security vendors, which causes clients to **question whether they can rely** on embedded security alone.

Take Advantage Today

SD WAN

SD-WAN Ready

- ✓ FortiGate provides best of breed SD-WAN features in base platform
- ✓ Make your branch application aware with our WAN Path Controller
- ✓ Consistent application performance with automated fail-over

NGFW

Proven NGFW

- ✓ 90% of SD-WAN vendors do not offer NGFW security
- ✓ Fortinet is the industry leader in Security Effectiveness and Performance
- ✓ Simple to manage integrated NGFW And SD-WAN in single offering

3rd Party Verification

FORTINET

Gartner MQ WAN Edge Infrastructure

Figure 1. Magic Quadrant for WAN Edge Infrastructure

Source: Gartner (October 2018)

NSS Labs

"NSS Labs, Inc. is recognized globally as the **most trusted source for independent, fact-based cybersecurity guidance**. Our mission is to advance **transparency** and accountability within the **cybersecurity industry**. We empower enterprises by providing them with timely, relevant information on which to base their decisions.

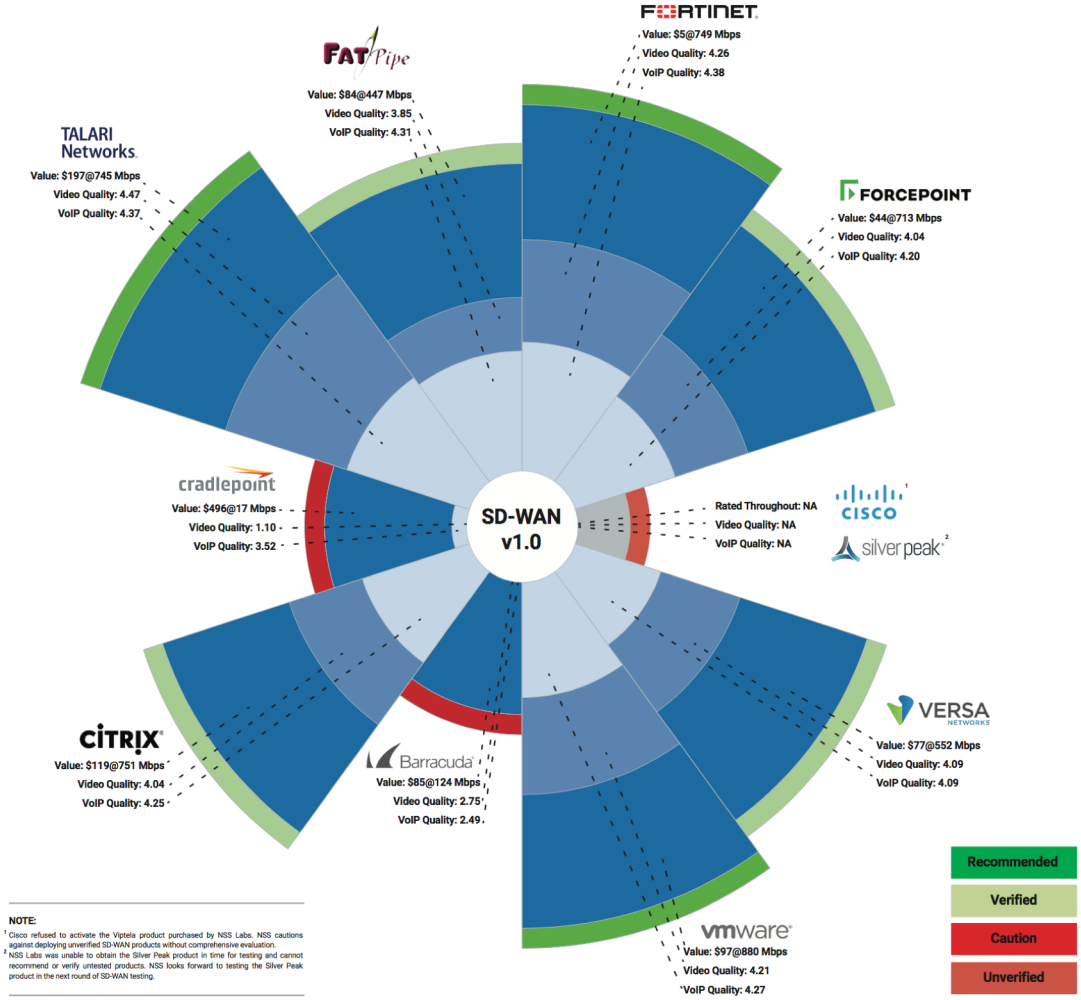
Our unmatched foundation in security testing, along with our extensive research and global threat analysis capabilities, provide the basis for our CAWS Continuous Security Validation Platform. CAWS measures the ongoing effectiveness of security controls, **providing a real-time score card to help business leaders substantiate their security investments**."

Recommended by NSS labs

- Fortinet is the only vendor with Security Capabilities to Receive SD-WAN Recommended Rating in the First NSS Labs Software-Defined Wide Area Networking Test Report

- **Highest quality of experience for VoIP**
  (4.38 out of 4.41)
- **Lowest total cost of ownership (TCO)**
  $5@749Mbps
- **Native NGFW Security**
  Blocked 100% Evasions

SD-WAN Value Map

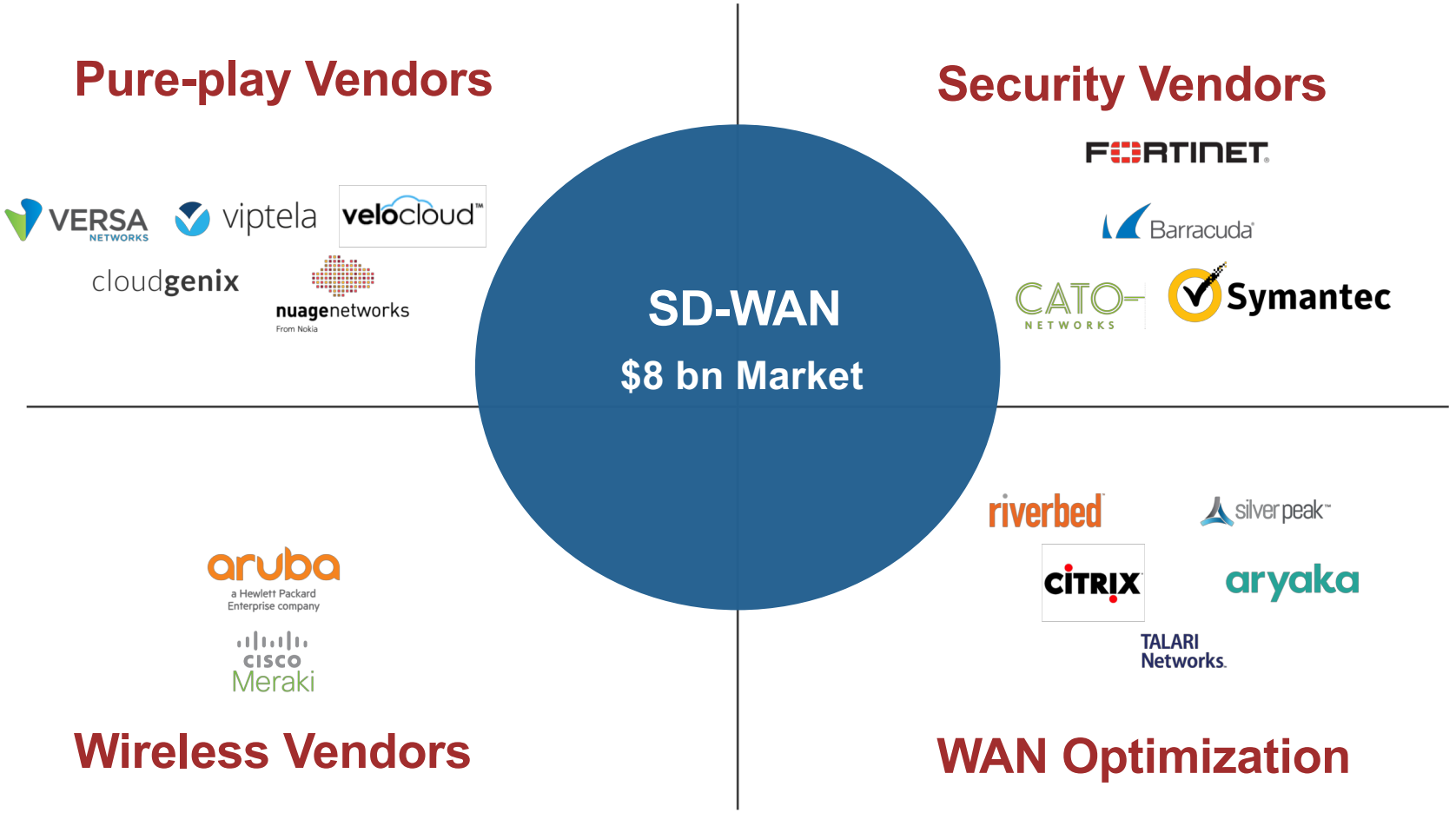


Vendor	QoE for VoIP		QoE for Video		TCO per Mbps	Overall Rating
Barracuda Networks	2.49	Below Use Case	2.75	Below Use Case	$85	Caution
Citrix Systems	4.25	Above Use Case	4.04	Above Use Case	$119	Verified
Cradlepoint	3.52	Above Use Case	1.10	Below Use Case	$496	Caution
FatPipe Networks	4.31	Above Use Case	3.85	Above Use Case	$84	Verified
Forcepoint	4.20	Above Use Case	4.04	Above Use Case	$44	Verified
Fortinet	4.38	Above Use Case	4.26	Above Use Case	$5	Recommended
Talari Networks	4.37	Above Use Case	4.47	Above Use Case	$197	Recommended
Versa Networks	4.09	Above Use Case	4.09	Above Use Case	$77	Verified
VMware	4.27	Above Use Case	4.21	Above Use Case	$97	Recommended

Competitive

FORTINET

Crowded SD-WAN Market



Only Fortinet delivers integrated Secure SD-WAN

Features	SD-WAN Vendors	Security Vendors	Combinations	Fortinet
SD-WAN				
NGFW Security				
Single Console				
Cost				

Why Fortinet has the best Secure SD-WAN solution?

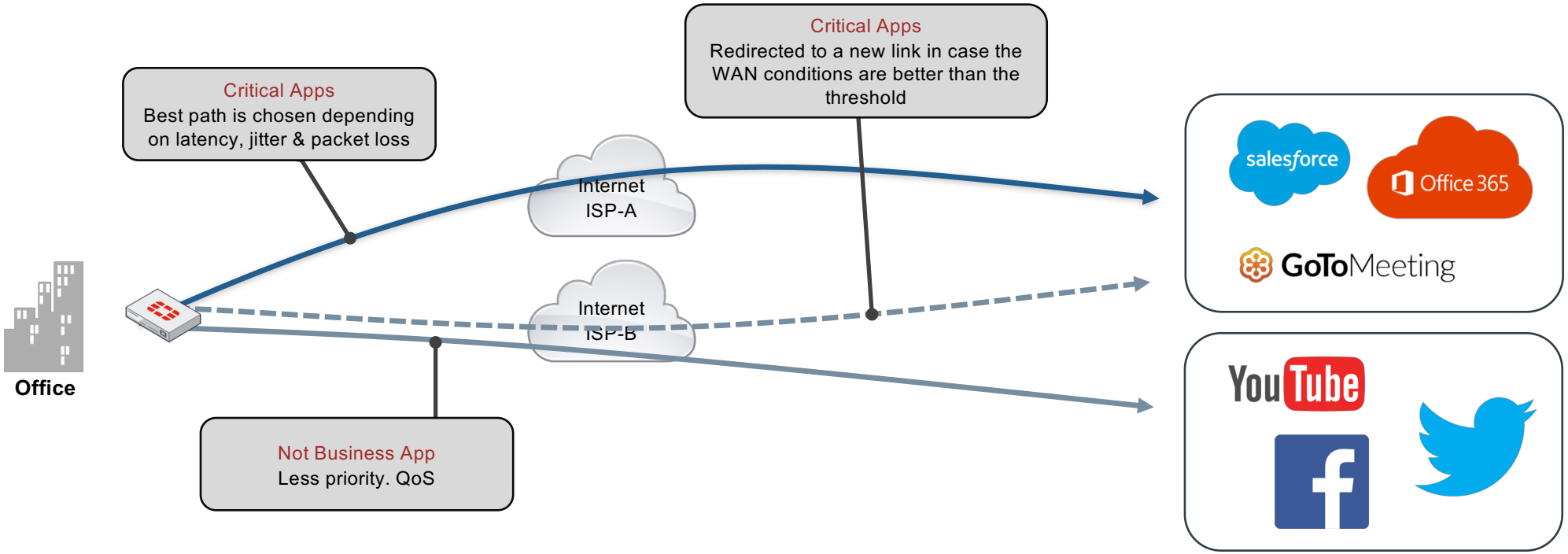
	Fortinet	Velocloud	Versa Networks	Cisco Viptela	Cisco Meraki	Cisco IWAN	Riverbed
WAN Path Controller w/ Application SLA							
NGFW w/SSL Inspection							
Application Awareness							
Dynamic Failover times							
Scalable Auto IPsec VPN Overlays							
Single Management Console for Security & SD-WAN							
Zero-touch Provisioning							
TCO							

SD-WAN Use Cases

FORTINET

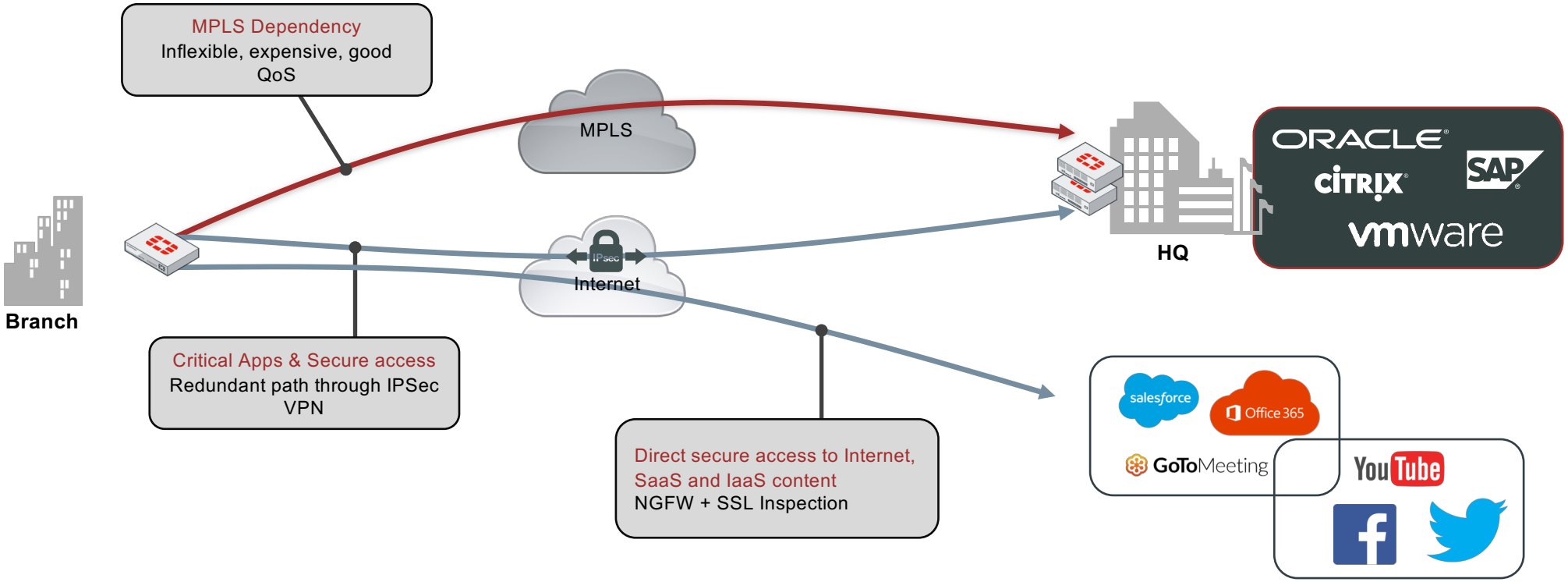
Enterprise SD-WAN Use Cases

Internet SaaS – Application Aware + Path Awareness Intelligence



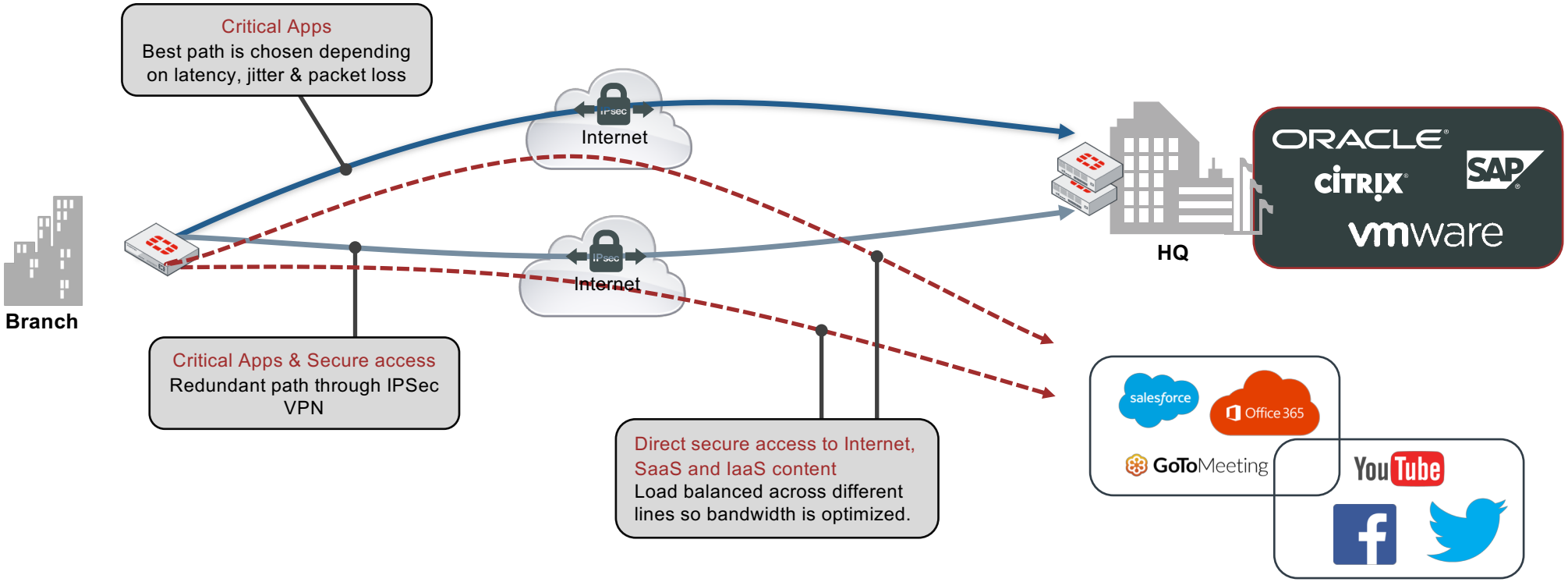
Enterprise SD-WAN Use Cases

MPLS backup with local breakout



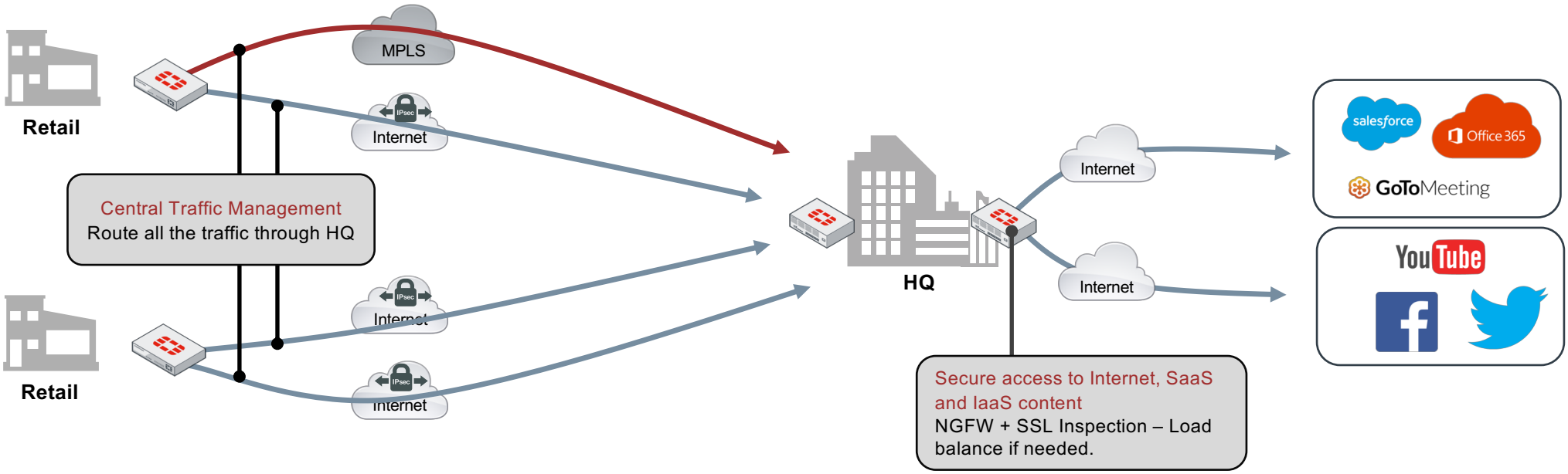
Enterprise SD-WAN Use Cases

MPLS replacement



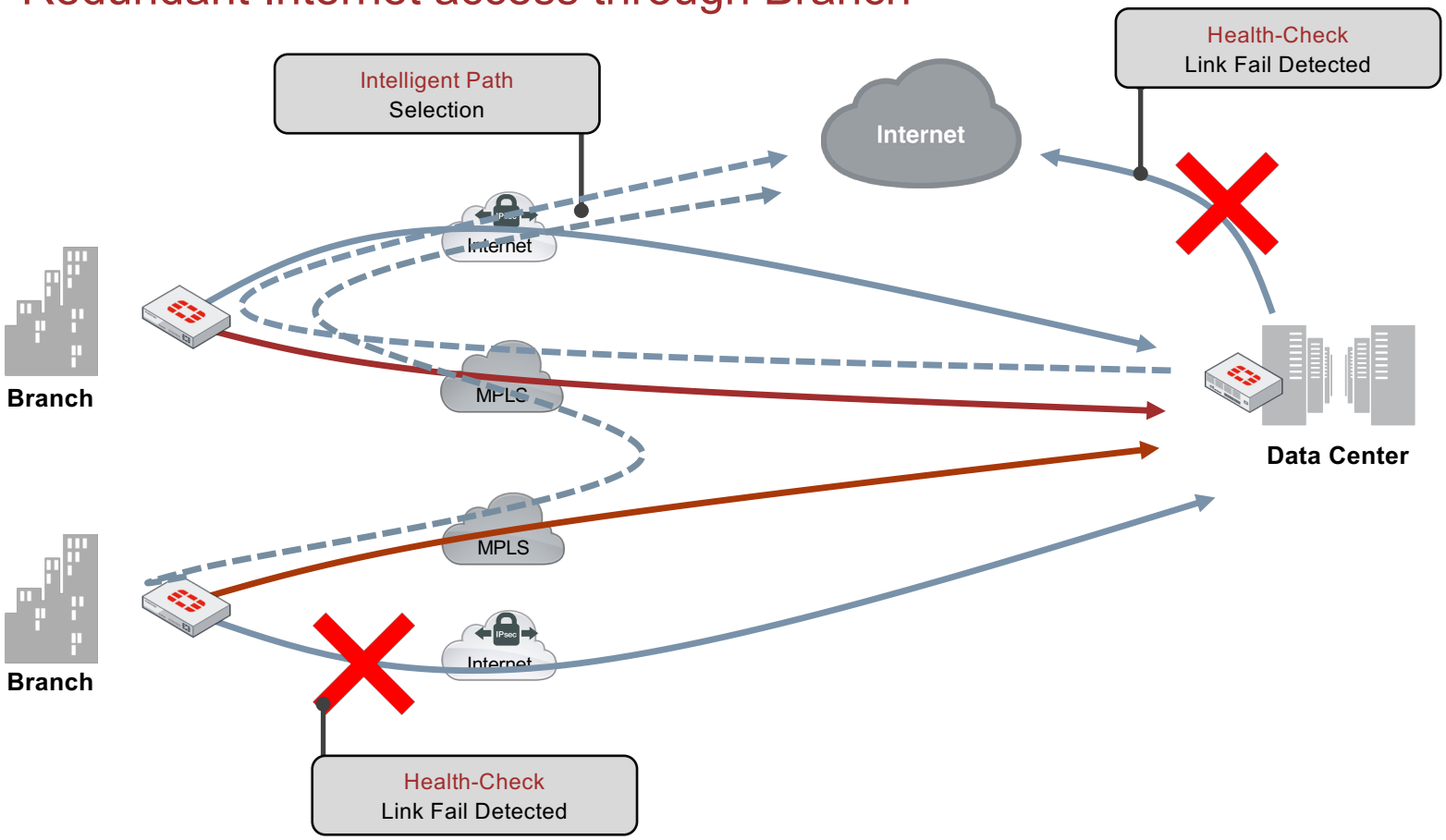
Enterprise SD-WAN Use Cases

Centralized Internet Management



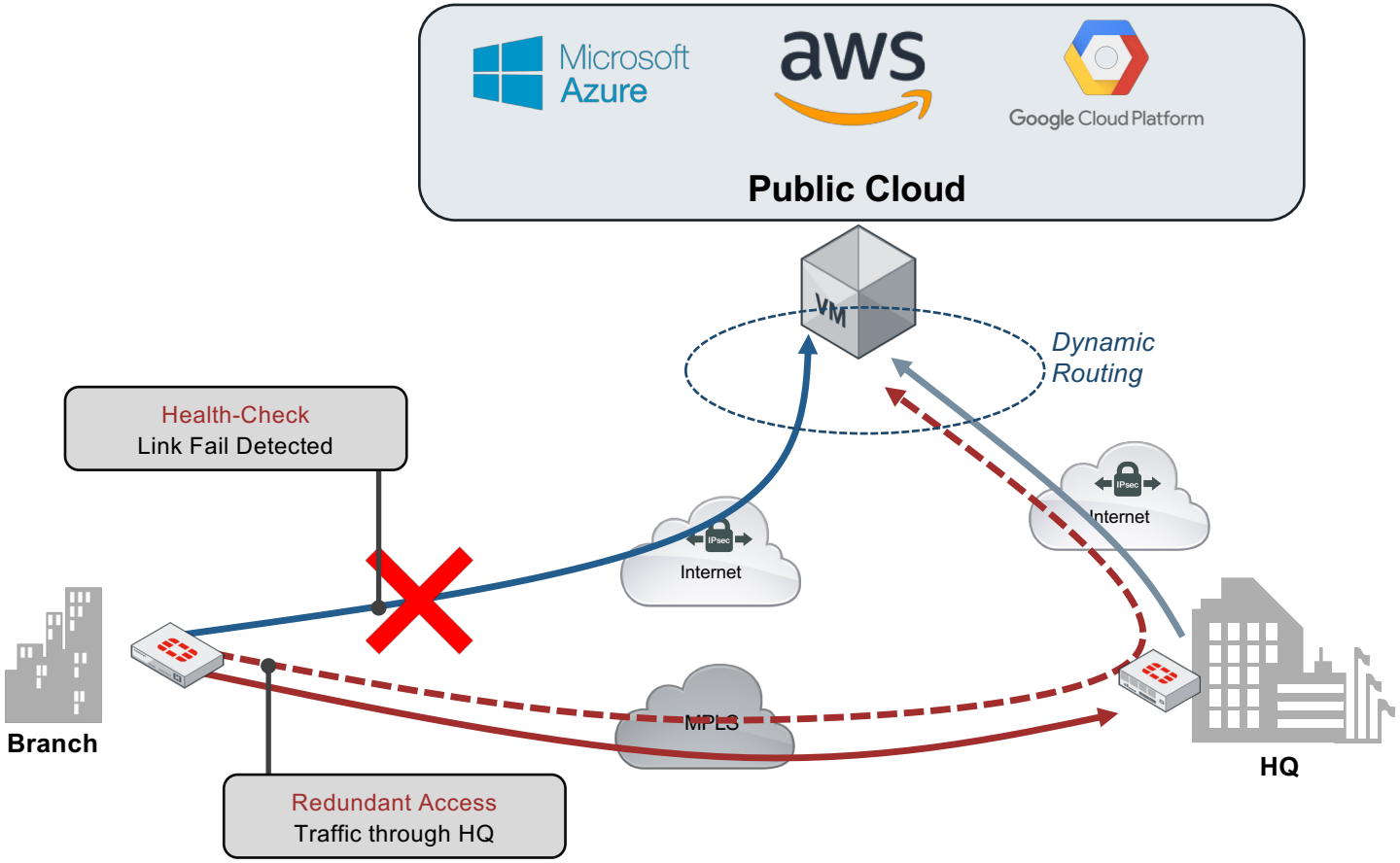
ISP SD-WAN Use Cases

Redundant Internet access through Branch



Enterprise SD-WAN Use Cases

Redundant Public Cloud access



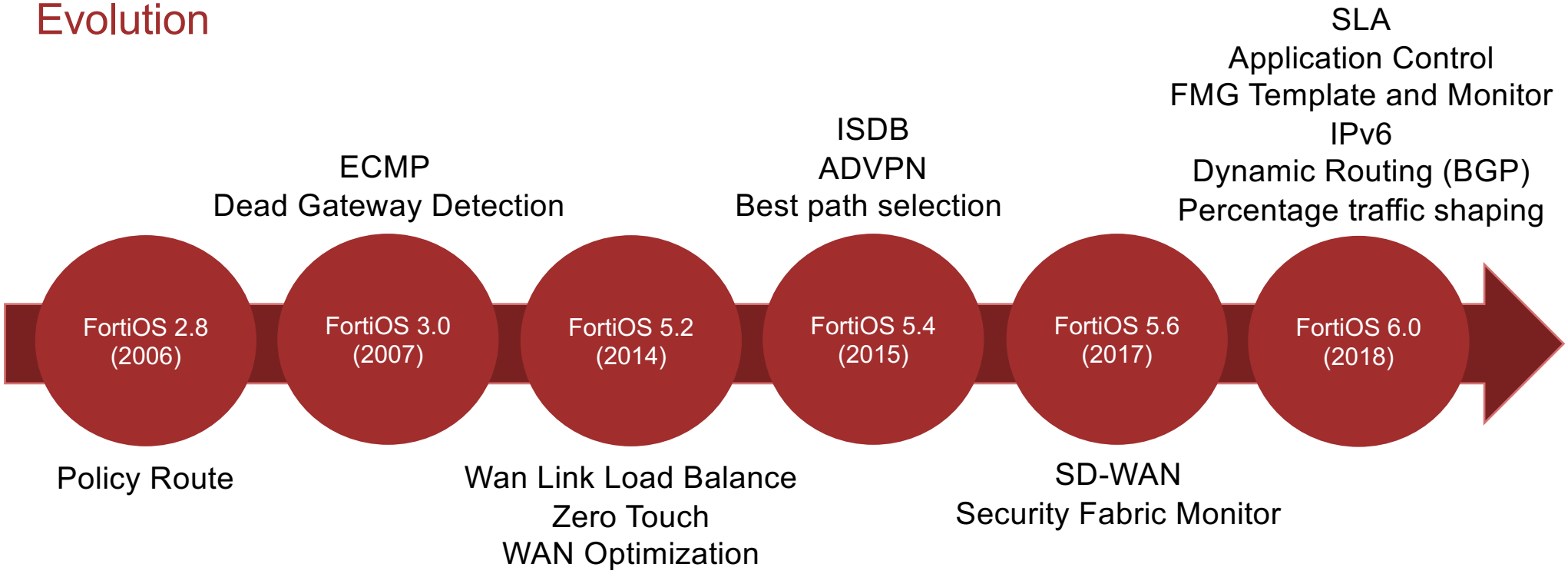
FortiOS SD-WAN

Technical Guide

FORTINET

FortiOS SD-WAN

Evolution



FortiOS SD-WAN

Evolution

	5.2	5.4	5.6	6.0
WAN link load balancing	✓	✓	✓	✓
Routing, QoS and WAN Optimization	✓	✓	✓	✓
ADVPN (Site to Site VPN)		✓	✓	✓
Best quality WAN path selection		✓	✓	✓
SD-WAN Controller replaces WAN LLB			✓	✓
FortiManager SD-WAN support			✓	✓
Application traffic shaping for SD-WAN			✓	✓
BGP Dynamic Routing for SD-WAN			✓	✓
Minimum SLA enforcement link steering				✓
Multiple SLAs per SD-WAN rule				✓
Set link preference in SD-WAN rule				✓
Auto failback to primary link				✓
Interface percentage based traffic shaping				✓
Expanded application signatures for steering (~3000 apps)				✓

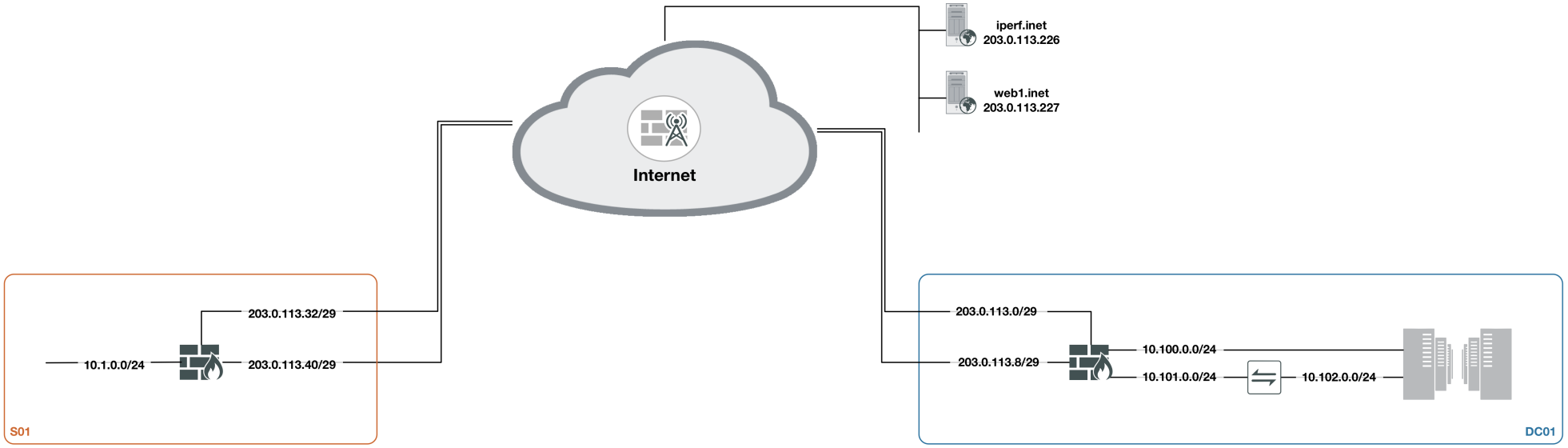
FortiOS SD-WAN

Basic Config Overview

FORTINET

Demo – Hub and Spoke

Network Diagram



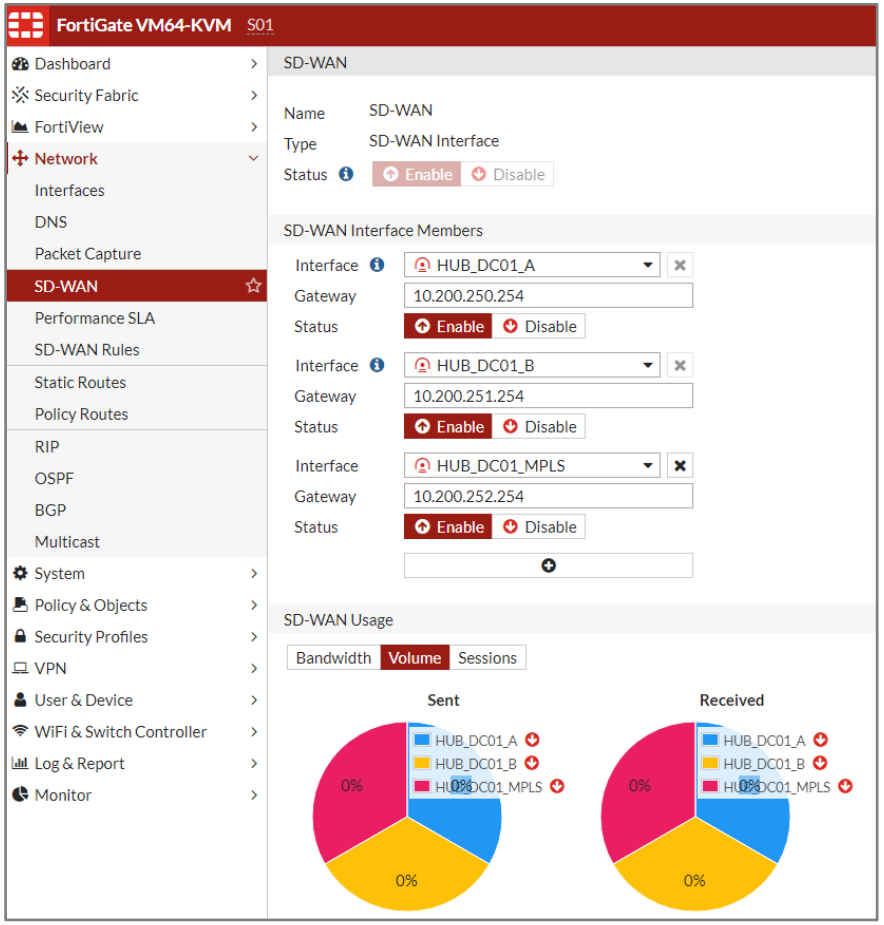
FortiOS SD-WAN

Basic Config Overview

FORTINET

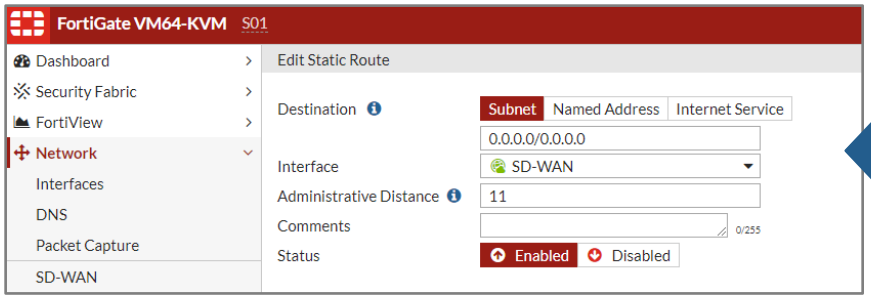
FortiOS SD-WAN

Basic Config - Interface Members



FortiOS SD-WAN

Basic Config - Static Routing



You need to add a route to SD-WAN interface to install the SD-WAN interface in the routing table. **Load balancing algorithm will not work otherwise**.

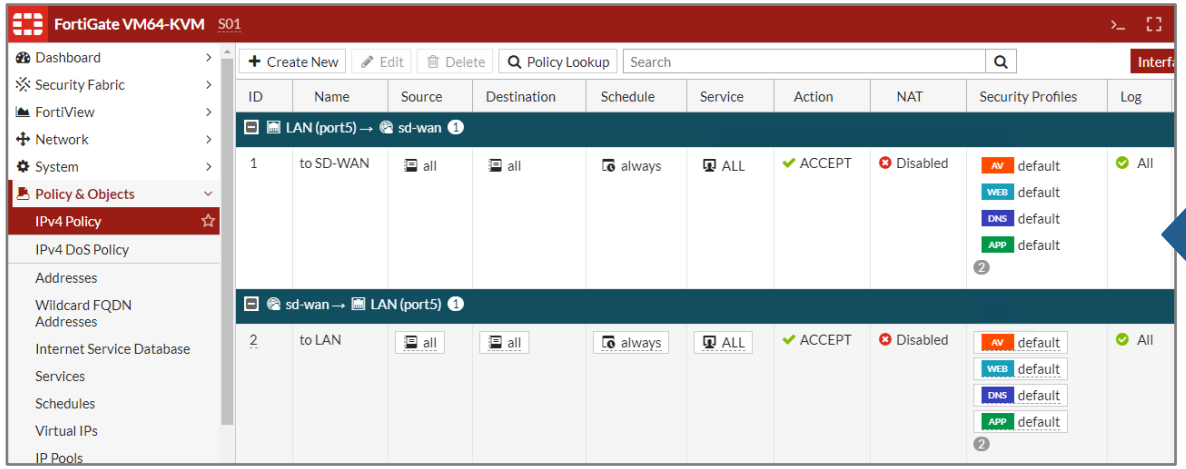
```
FG # get router info routing-table all
Routing table for VRF=0
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [1/0] via 192.168.0.1, wan1, [0/55]
                  [1/0] via 200.225.196.247, ppp1, [0/3]
```

FortiGate automatically add the Default Gateway addresses from SD-WAN interface configuration

FortiOS SD-WAN

Basic Config - Firewall Policy



sd-wan *virtual interface will be available as source interface and destination interface in Firewall Policy*

Aggregate multiple interfaces into a single SD-WAN interface and apply a security policy across all.

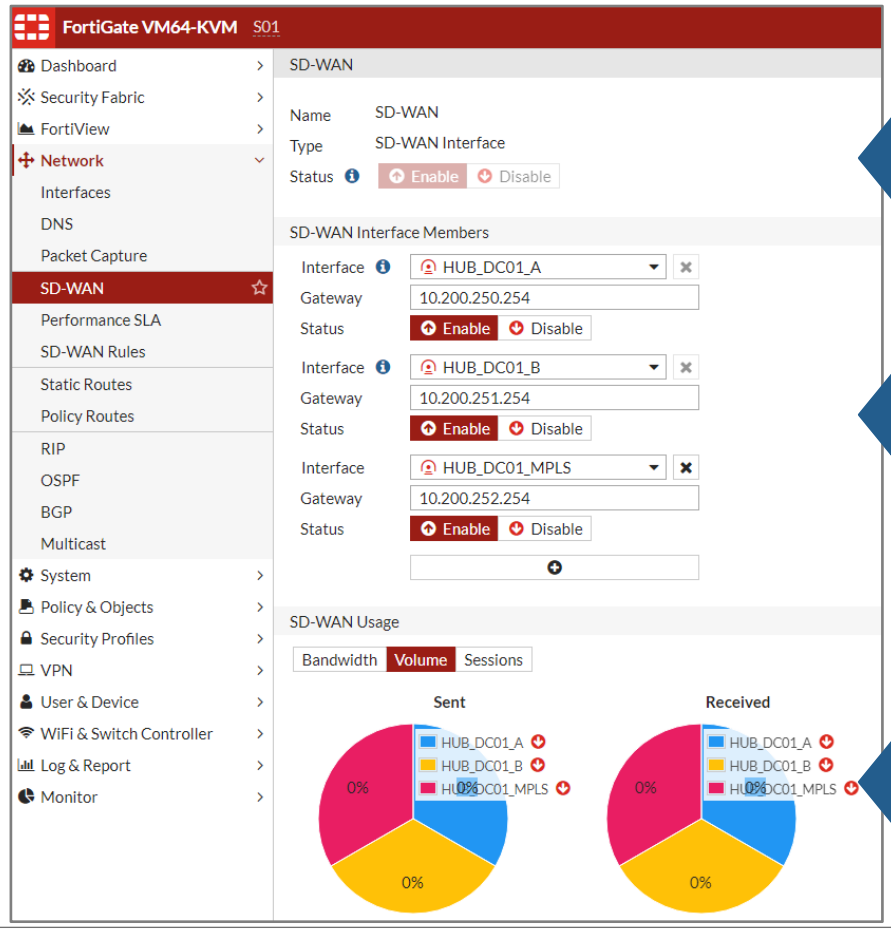
FortiOS SD-WAN

SD-WAN Interface

FORTINET

FortiOS SD-WAN

Interface Members



Enable or Disable the **sd-wan** virtual interface

Configure all **Interfaces** and **Gateways** members that will be used in SD-WAN
Support physical, VLAN, IPSec, 3G/4G and FortiExtender interfaces

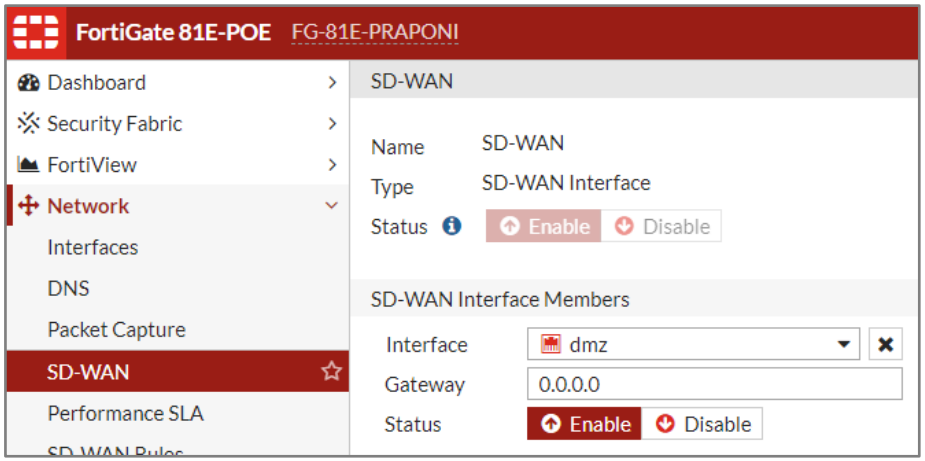
SD-WAN usage dashboard. Statistics only

FortiOS SD-WAN

IPv6 Interface Members

```
config system virtual-wan-link
    set status enable
    config members
      edit 1
        set interface "dmz"
        set gateway6 2004:10:100:1::1
      next
    end
end
```

IPv6 link configuration in SD-WAN is CLI only.
Setting **gateway6** parameter.



In the GUI, the **Gateway** config is displayed as **0.0.0.0** for IPv6

FortiOS SD-WAN

Interface Members

```
config system virtual-wan-link
    config members
      edit wan1
        set gateway 192.168.0.1
        set source 0.0.0.0
        set gateway6 ::
        set source6 ::
        set priority 0
        set weight 0
        set volume-ratio 0
        set spillover-threshold 0
        set ingress-spillover-threshold 0
      next
    end
end
```

- **gateway**: IPv4 gateway
- **source**: IPv4 address used in the health-check packet to the server. If 0.0.0.0 interface address will be used
- **gateway6**: IPv6 gateway
- **source6**: Same as source but for IPv6
- **priority**: Used for SD-WAN rules or priority rules
- **weight**: Weight of this interface for weighted load balancing. More traffic is directed to interfaces with higher weights
- **volume-ratio**: Measured volume ratio (this value / sum of all values = percentage of link volume)
- **spillover-threshold**: Egress spillover threshold for this interface. When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN
- **ingress-spillover-threshold**: Ingress spillover threshold for this interface. When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN

** weight, volume-ratio, spillover-threshold, ingress-spillover-threshold it is displayed based on **load-balance-mode** configuration*

FortiOS SD-WAN

Interface Bandwidth

```
config system interface
    edit wan1
        set inbandwidth 10000
        set outbandwidth 20000
        set estimated-upstream-bandwidth 20000
        set estimated-downstream-bandwidth 10000
    next
end
```

inbandwidth/outbandwidth (kbps) needs be configured for SD-WAN Rule usage as Downstream, Upstream and Bandwidth - Best Quality options

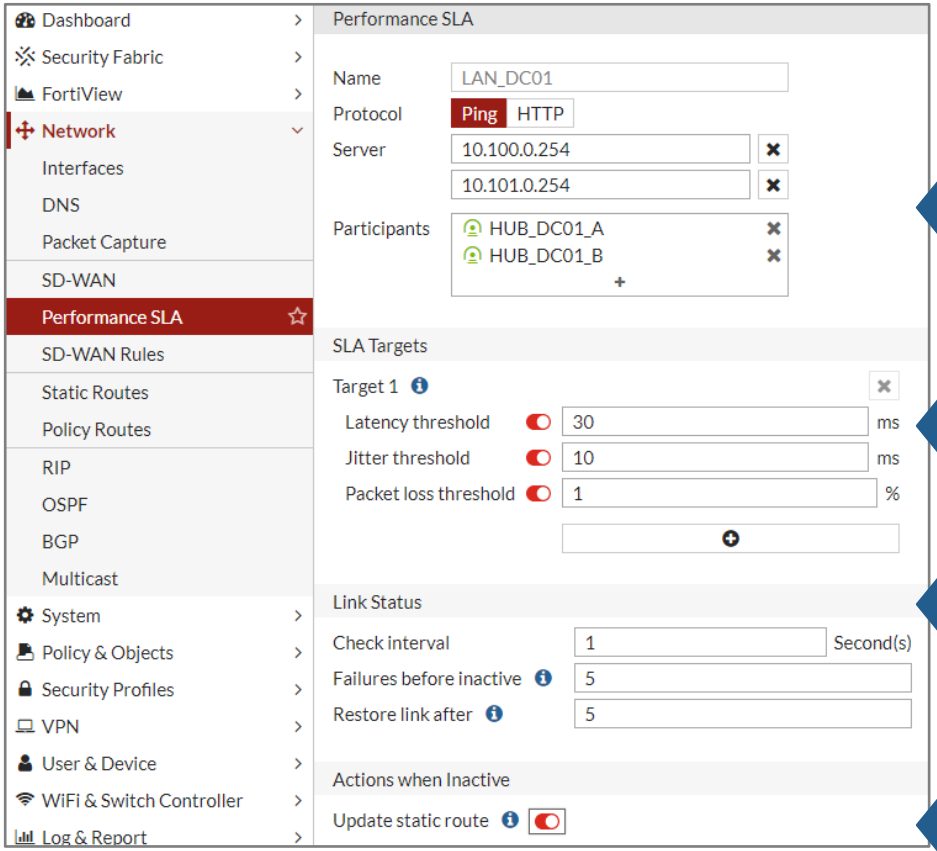
estimated-upstream-bandwidth / estimated-downstream-bandwidth (kbps) used to estimate link utilization on GUI

FortiOS SD-WAN

Performance SLA

FortiOS SD-WAN

Performance SLA



***Protocol**: Use **ping** or **http** to test the link with the server*
***Server**: IP address or FQDN name of the server. If two servers are configured, both needs fail to link be detected as offline*
***Participants**: Interfaces members for this health-check*

SLA Targets (optional). Used in SD-WAN Rule SLA Strategy

*Status **check interval**, or the time between attempting to connect to the server*
*Number of **failures** before server is considered lost*
*Number of successful responses received before server is considered **recovered***

*Enable/disable **updating the static route***
When enabled and health-check fail, FortiOS will disable static routes for inactive interfaces

FortiOS SD-WAN

Performance SLA

```
config system virtual-wan-link
    config health-check
      edit "test-link"
        set addr-mode    : ipv4 | ipv6
        set server       : "1.1.1.1"
        set protocol     : ping
        set interval     : 2
        set failtime     : 5
        set recoverytime     : 5
        set update-cascade-interface: enable
        set update-static-route : disable
        set threshold-warning-packetloss: 0
        set threshold-alert-packetloss: 0
        set threshold-warning-latency: 0
        set threshold-alert-latency: 0
        set threshold-warning-jitter: 0
        set threshold-alert-jitter: 0
        set members      : 1 2
      next
    end
end
```

- ***addr-mode***: *Address mode (IPv4 or IPv6)*
- ***server***: *configure multiple servers in SD-WAN health-check*
- ***protocol***: *Support ping, tcp-echo, udp-echo, http, twamp and ping6 to test the link with the server*
- ***interval***: *Status check interval, or the time between attempting to connect to the server*
- ***failtime***: *Number of failures before server is considered lost*
- ***recoverytime***: *Number of successful responses received before server is considered recovered*
- ***update-cascade-interface***: *Enable to bring down the source interface if the link health monitor fails.*
- ***update-static-route***: *Enable to remove static routes from the routing table that use this interface if the link monitor fails*
- ***threshold-warning-packetloss***: *Warning threshold for packet loss (%)*
- ***threshold-alert-packetloss***: *Alert threshold for packet loss (%)*
- ***threshold-warning-latency***: *Warning threshold for latency (ms)*
- ***threshold-alert-latency***: *Alert threshold for latency (ms)*
- ***threshold-warning-jitter***: *Warning threshold for jitter (ms)*
- ***threshold-alert-jitter***: *Alert threshold for jitter (ms)*
- ***members***: *Member sequence number list*

FortiOS SD-WAN

Performance SLA - HTTP protocol

```
config system virtual-wan-link
    config health-check
      edit "test-link"
        ...
        set server  : "www.google.com"
        set protocol  : http
        set port  : 80
        set http-get   : /
        set http-match   :
        ...
      next
    end
end
```

- ***protocol:*** *http*
- ***port:*** *Port number used to communicate with the server over the selected protocol*
- ***http-get:*** *URL path used to communicate with the server if the protocol if the protocol is HTTP*
- ***http-match:*** *Response string expected from the server if the protocol is HTTP. Use blank to accept any*

FortiOS SD-WAN

Performance SLA - TWAMP protocol (CLI Only)

Client-Side

```
config system virtual-wan-link
    config health-check
      edit "test-link"
        ...
        set server   : 192.168.30.1
        set protocol   : twamp
        set security-mode   : authentication
        set password: fortinet
        set packet-size    : 64
        set port: 8008
        ...
```

- ***protocol:*** *twamp*
- ***port:*** *Port number used to communicate with the server over the selected protocol*
- ***security-mode:*** *Twamp controller security mode {none | authentication}*
- ***password****: Twamp controller password in authentication mode*
- ***packet-size:*** *Packet size of a twamp test session*

Server-Side

```
config system probe-response
    set mode twamp
end
```

*Configure system **probe-response** with **twamp** mode in FortiGate Server*

** Remember to configure allowaccess "**probe-response**" on interface of TWAMP Client and Server communication*

FortiOS SD-WAN

Performance SLA - SNMP Support

```
FG # diag sys virtual-wan-link health-check
Health Check(ping):
Seq(1): state(alive), packet-loss (0.000%) latency (0.381), jitter(0.024) sla_map=0x0
Seq(2): state(alive), packet-loss (0.000%) latency (0.700), jitter(0.084) sla_map=0x0
```

```
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkState.1 = INTEGER: alive(0)
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkState.2 = INTEGER: alive(0)
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkLatency.1 = STRING: 0.381
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkLatency.2 = STRING: 0.700
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkJitter.1 = STRING: 0.024
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkJitter.2 = STRING: 0.084
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkPacketSend.1 = Counter64: 8409
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkPacketSend.2 = Counter64: 8409
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkPacketRecv.1 = Counter64: 8359
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkPacketRecv.2 = Counter64: 8336
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkPacketLoss.1 = STRING: 0.000
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkPacketLoss.2 = STRING: 0.000
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkVdom.1 = STRING: root
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkVdom.2 = STRING: root
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkBandwidthIn.1 = Counter32: 100
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkBandwidthIn.2 = Counter32: 100
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkBandwidthOut.1 = Counter32: 100
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkBandwidthOut.2 = Counter32: 100
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkBandwidthBi.1 = Counter32: 200
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkBandwidthBi.2 = Counter32: 200
```

Same results from CLI you can get from a SNMP client with FortiGate-MIB

FortiOS SD-WAN

Performance SLA - SNMP Support

Description	Value
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkState	.1.3.6.1.4.1.12356.101.4.9.2.1.4
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkLatency	.1.3.6.1.4.1.12356.101.4.9.2.1.5
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkJitter	.1.3.6.1.4.1.12356.101.4.9.2.1.6
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkPacketSend	.1.3.6.1.4.1.12356.101.4.9.2.1.7
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkPacketRecv	.1.3.6.1.4.1.12356.101.4.9.2.1.8
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkPacketLoss	.1.3.6.1.4.1.12356.101.4.9.2.1.9
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkBandwidthIn	.1.3.6.1.4.1.12356.101.4.9.2.1.11
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkVdom	.1.3.6.1.4.1.12356.101.4.9.2.1.10
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkBandwidthOut	.1.3.6.1.4.1.12356.101.4.9.2.1.12
FORTINET-FORTIGATE-MIB::fgVWLHealthCheckLinkBandwidthBi	.1.3.6.1.4.1.12356.101.4.9.2.1.13

FortiOS SD-WAN

Performance SLA – Best Practices

Customers like to see fast failovers!

- For PoC's, always use low values in **Check Interval** and **Failures before inactive**
  - » The same for IPSec VPN Phase 1 **dpd-retrycount** and **dpd-retryinterval**
- Use at least 5 retries in **Restore link after** to avoid link flapping
- If "set source" is not configured in CLI, interface IP will be used for health checks
  - » If the interface does not have an IP this could lead to unexpected results

FortiOS SD-WAN

Performance SLA – Best Practices

- Configure '**update-static-route disable**' if you have a Health Check that, even if isn't reachable, will not prevent the path to other networks associated to that interface, e.g. when you have a HC to a DataCenter Switch Core but even if the SW Core is down you still should be able to reach the DC FW LAN interfaces

- Packet Loss use the last 30 samples to calculate it's average value
- In a Hub-and-Spoke topology, use FortiGate interface as Detection Server

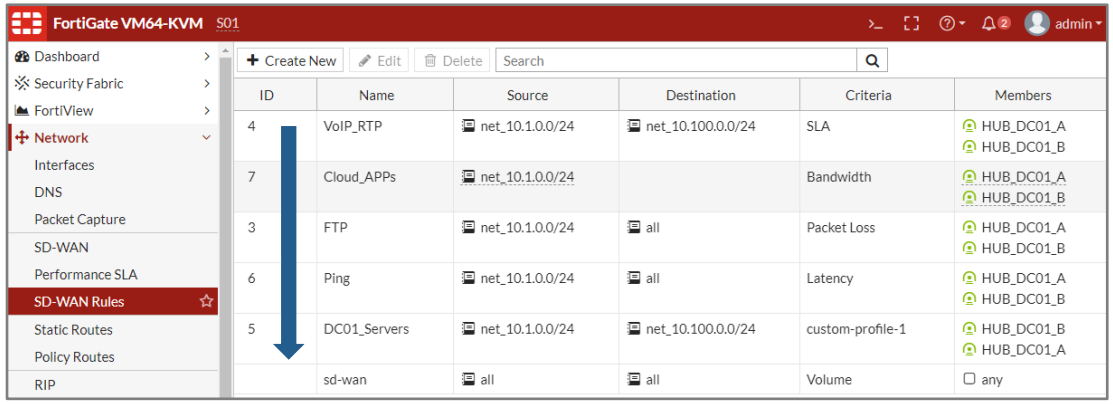
FortiOS SD-WAN

SD-WAN Rules

FORTINET

FortiOS SD-WAN

Rules

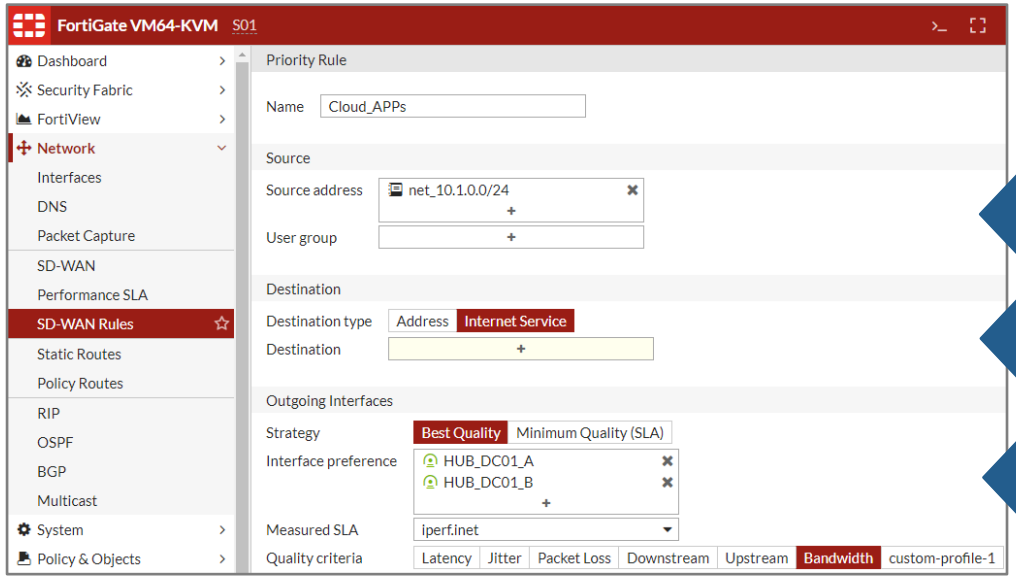


- SD-Wan rules are top down. The order is important
- If no rule match, the implicit rule will be used
- Each rule is a “policy route” inside FortiOS

The traffic will be load balanced only in implicit rule

FortiOS SD-WAN

Rules



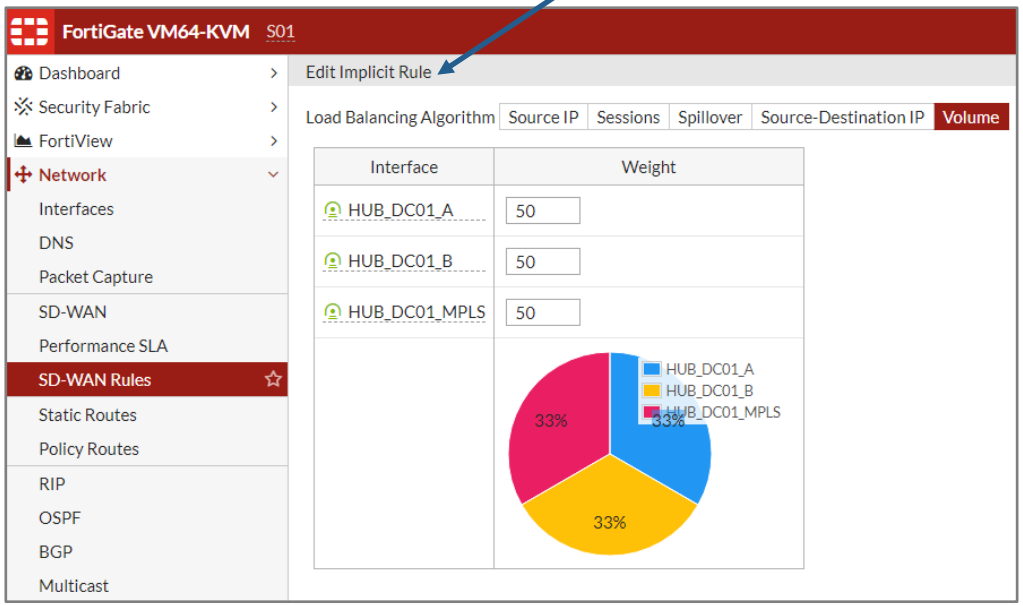
Source (optional) fields. Accept IP/Mask and User Group

Destination address, protocol, Internet Service and Application Control

Outgoing interfaces can be selected based on Best Quality, Minimum Quality (SLA) and manual (CLI only)

FortiOS SD-WAN

Rules – Implicit Rule



Implicit catch all the bottom decides how to distribute remainder of traffic:

- Source IP
- Sessions
- Spillover
- Source-Destination
- Volume

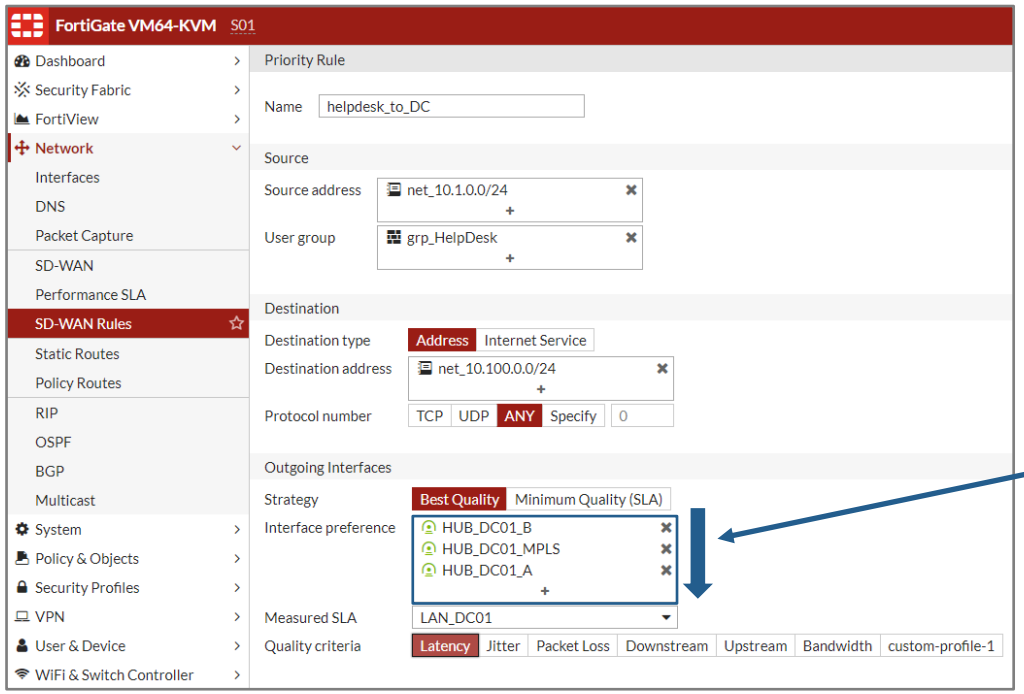
FortiOS SD-WAN Rules – Implicit Rule Algorithms

How it works?

- Source IP
  - The source IP algorithm tries to equally divide the traffic between the interfaces included in the virtual WAN interface. It use the connection criteria of the source IP address as a way of sorting the traffic.
- Sessions
  - The session algorithm uses an integer value to assign a weight to each interface. The difference is that the number of sessions connected is what is being measured and not the packets flowing through the interfaces.
- Spillover
  - Spillover is a method where a threshold is set for an interface (in kbps) and if the amount of traffic bandwidth exceeds the threshold any traffic bandwidth beyond that threshold is sent out through another interface.
- Source-Destination
  - The source-destination IP algorithm tries to equally divide the traffic between the interfaces included in the virtual WAN interface. It use the connection criteria of the source and destination IP address combinations as a way of sorting the traffic.
- Volume
  - This is a very straight forward method of distributing the work load based on the amount of packets going through the interfaces. An integer value assigns a weight to each interface. These weights are used to calculate a percentage of the total volume that is directed to the interface.

FortiOS SD-WAN Rules

Best Quality



The **Best Quality** Strategy:

FortiGate use the link providing the best network quality based on Latency, Jitter, Packet Loss, Downstream, Upstream, Bandwidth and custom-profile

When the difference between two links is within the amount that you configure for the **link-cost-threshold** (CLI) %, the FortiGate uses the link with the higher priority, which is the first member in the priority-members list

```
config system virtual-wan-link
    config health-check
      edit "test-link"
        set link-cost-threshold 10
    ...
```

FortiOS SD-WAN Rules

link-cost-threshold - How it works ?

```
set link-cost-threshold {integer}   Percentage threshold
change of link cost values that will result in policy
route regeneration (0 - 10000000, default = 10).
```

Purpose of the link cost threshold is to **prevent flapping** between networks so that if a fail-over happens, fail-back will only occur once the recovering network is 10% (default) better than the current network. Reason for the > 100 value is that some times you may want to only switch we need to switch back the route when member WAN1 quality is 5 times better of WAN2. So we might need to configure link-cost-factor as 500.

latency-threshold / jitter-threshold / packetloss-threshold are *only* used when a Best Quality strategy is set. This is the measurement trigger used to **decide if an interface is out of SLA** i.e. If latency-threshold = 100ms and it is actually 150ms, the interface is out of SLA and fails for that health check.

FortiOS SD-WAN Rules – Best Quality

Best Quality – How it works ?

- Latency
  - » Select link based on (smaller) latency
- Jitter
  - » Select link based on (smaller) jitter
- Packet Loss
  - » Select link based on (smaller) packet loss
- Downstream*
  - » Select link based on available bandwidth from download usage
- Upstream*
  - » Select link based on available bandwidth from upload usage
- Bandwidth*
  - » Select link based on available bandwidth from download and upload usage

For *Downstream, Upstream and Bandwidth the value is based on "inbandwidth/outbandwidth" in interface setting. If not set, will use physical speed minus current usage.*

FortiOS SD-WAN Rules – Best Quality

Use Cases

- Latency
  - How much time it takes for a packet of data to get from one designated point to another.
  - Less Latency = Better throughput
  - Issues: Slow access, connection failure
  - Recommended for applications that require best response time. Example: Video/VoIP

- Jitter
  - Is the variance in time delay in milliseconds (ms) between data packets over a network. It is a disruption in the normal sequence of sending data packets. Jitter is generally caused by congestion in the IP network
  - Issues: Delay in real time applications
  - Recommended for application that require effective packet delivery. Example: VoIP

FortiOS SD-WAN Rules – Best Quality

Use Cases

- Packet Loss
  - » Occurs when one or more packets of data travelling across a computer network fail to reach their destination.
  - » Issues: Out-of-date information, slow loading times, loading interruptions, Closed connections and missing information.
  - » Recommended: Client-Server applications like Oracle DB and SSH

- Downstream
  - » Process of copying data from another computer over a network
  - » Issues: Slow access
  - » Recommended: Applications that needs network resources to download data. Example: File Server, Cloud Storage (Dropbox, OneDrive)

FortiOS SD-WAN Rules – Best Quality

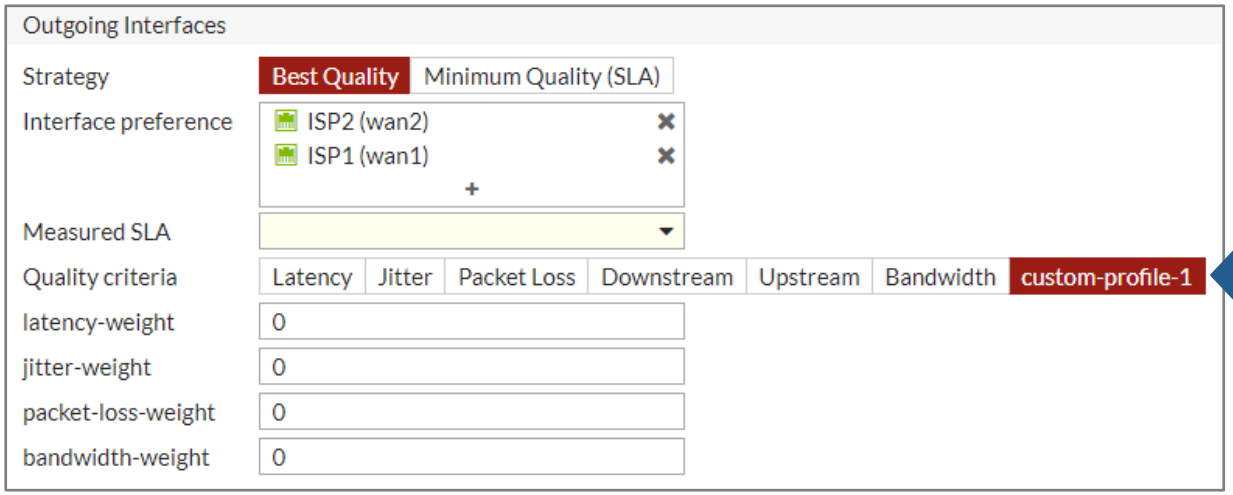
Use Cases

- Upstream
  - » Process of copying data to another computer over a network
  - » Issues: Slow transfer times, unable to complete upload
  - » Recommended: Applications that needs network resources to upload data. Example: Backup systems

- Bandwidth
  - » Sum of downstream + upstream
  - » Recommended: Applications that needs network resources to upload and download data. Example: File Server, Cloud Storage (Dropbox, OneDrive)

FortiOS SD-WAN Rules

Best Quality – Custom Profile



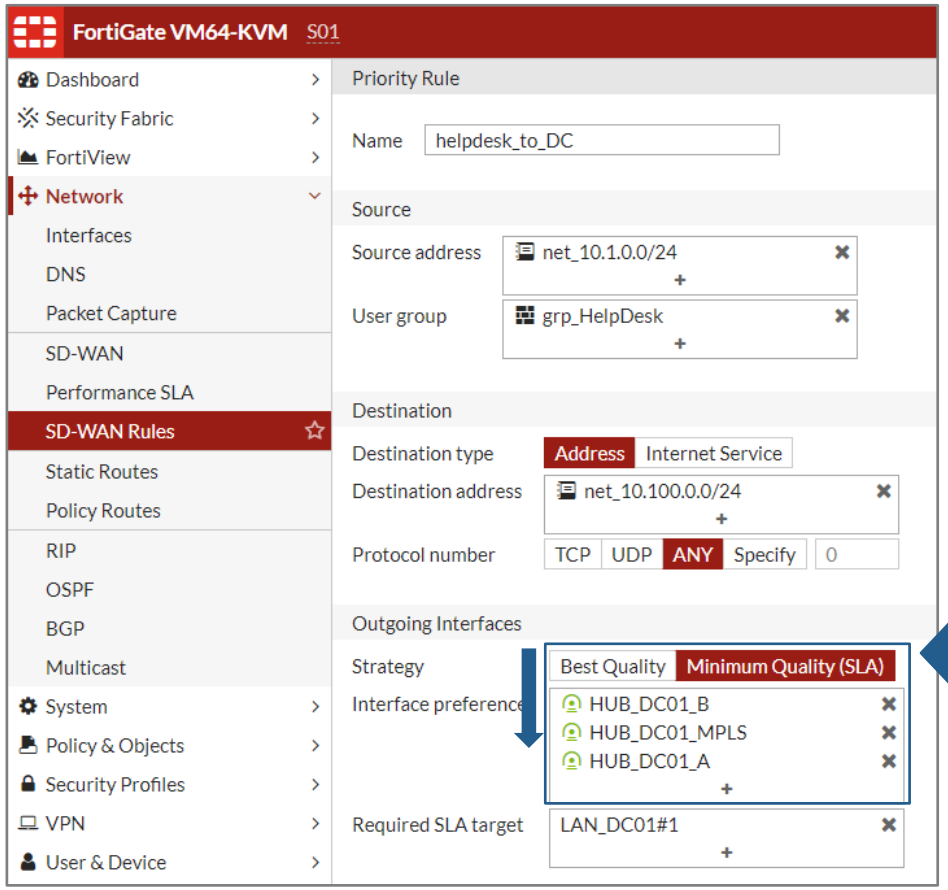
custom-profile1 calculates the best link using the following formula (useful for micro-managing the most critical applications flowing in an enterprise network).

- **latency-weight** - Coefficient of latency in the formula
- **jitter-weight** - Coefficient of jitter in the formula
- **packet-loss-weight** - Coefficient of packet-loss in the formula
- **bandwidth-weight** - Coefficient of reciprocal of available bidirectional bandwidth in the formula

Link Quality Index = (packet-loss-weight * packet loss) + (latency-weight * latency) + (jitter-weight * jitter) + (bandwidth-weight / bandwidth)

FortiOS SD-WAN Rules

Minimum Quality (SLA)



The **Minimum Quality (SLA)** strategy for SD-WAN:

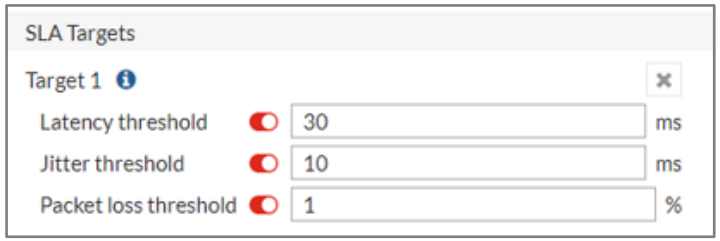
FortiGate will choose the best link for outgoing traffic based on SLA Targets profile

If all links meet the SLA criteria, the FortiGate uses the first link, even if that link isn't the best quality link. If at any time, the link in use doesn't meet the SLA criteria, and the next link in the configuration meets the SLA criteria, the FortiGate changes to that link. If the next link doesn't meet the SLA criteria, the FortiGate uses the next link in the configuration if it meets the SLA criteria, and so on.

FortiOS SD-WAN

Minimum Quality (SLA)

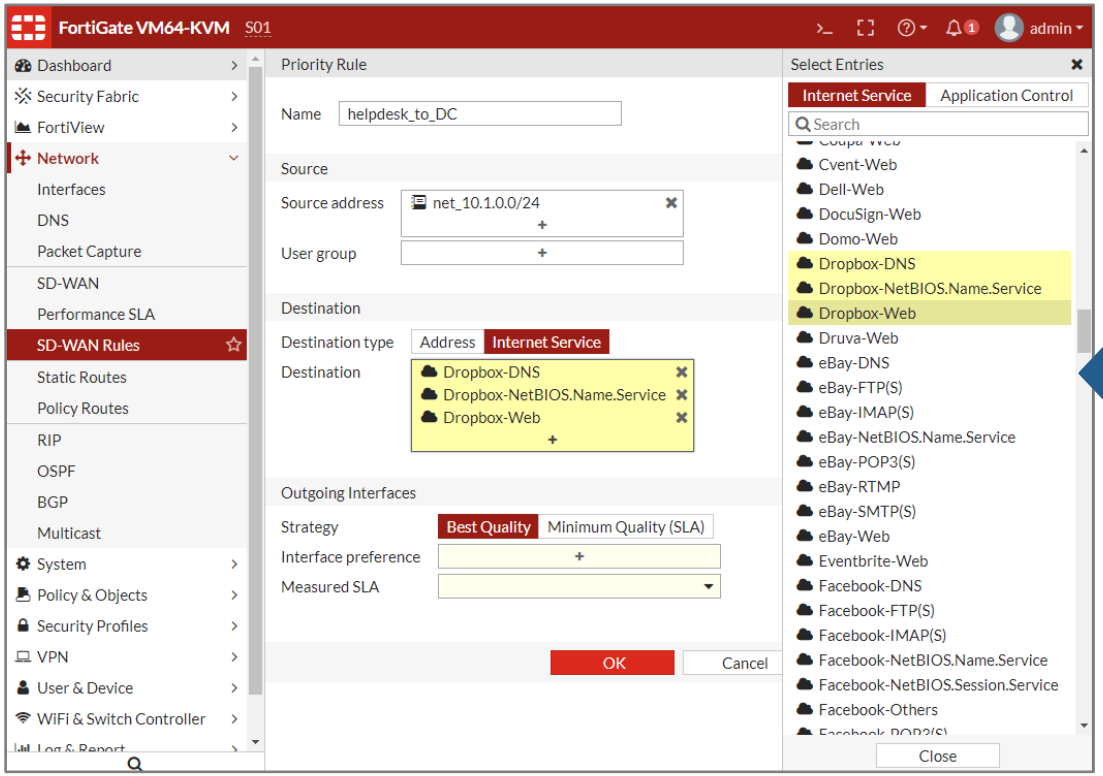
```
config system virtual-wan-link
    config health-check
      edit "test-link"
        ...
        config sla
          edit 1
            set link-cost-factor
            set latency-threshold 200
            set jitter-threshold 100
            set packetloss-threshold 3
          end
        end
      ...
end
```



- **link-cost-factor**: Criteria on which to base link selection
  - latency | jitter | packet-loss
- **latency-threshold**: Latency for SLA to make decision in milliseconds
- **jitter-threshold**: Jitter for SLA to make decision in milliseconds
- **packetloss-threshold**: Packet loss for SLA to make decision in percentage

FortiOS SD-WAN Rules – ISDB

Rules – Internet Service Database



Internet Service Database

- Dynamically updated (by FortiGuard) database of known service IPs and protocols
- Layer 4

ISDB as Rule **Destination**

FortiOS SD-WAN

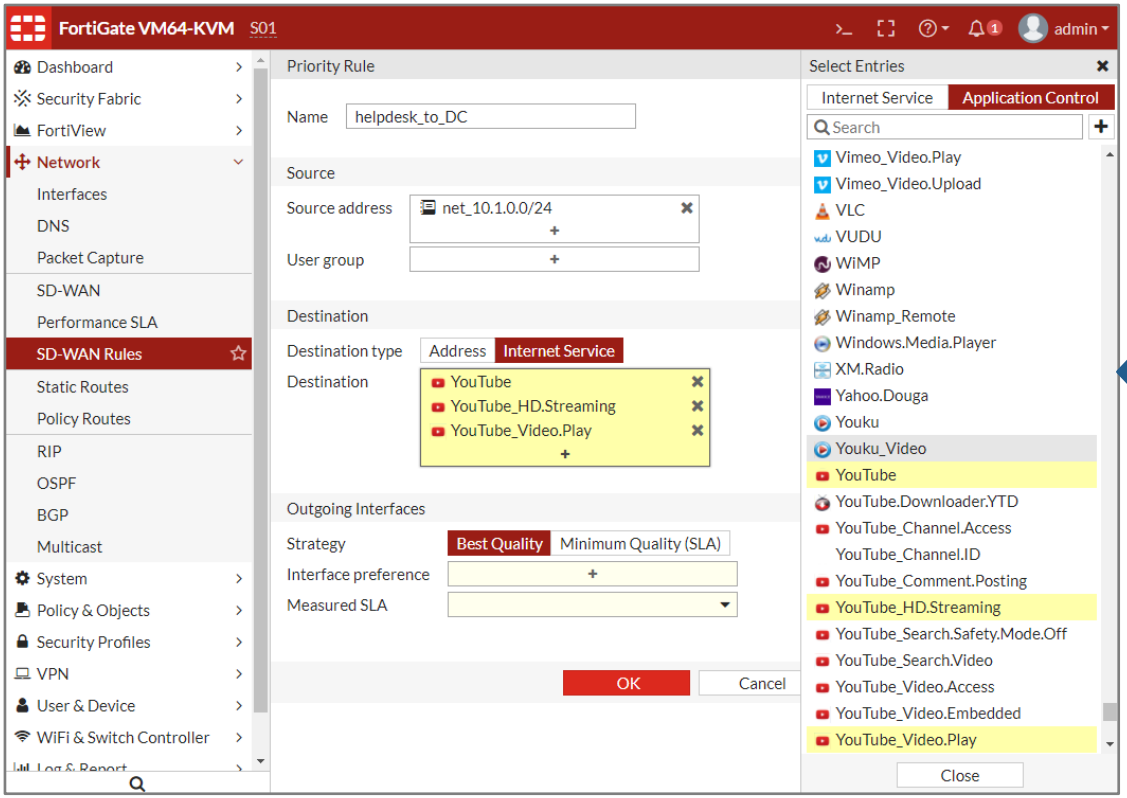
Rules – Internet Service Database

- Discover Internet Service name by IP

```
FG # diagnose internet-service match root 8.8.8.8 255.255.255.255
Internet Service: 65537(Google-Web), matched num: 2
Internet Service: 65539(Google-DNS), matched num: 1
```

FortiOS SD-WAN Rules – Application Control

Rules – Application Control



Application Control

- Dynamically updated database of applications
- Deep inspection
- Layer 7

2100+ Application Signatures (Layer 7) to use as **Destination**

FortiOS SD-WAN Rules – Application Control

Rules – Application Control - How it works?

- You need to add an Application Control profile in a firewall policy
- After the first packets are detected by Application Control engine, FortiOS will create a local, dynamic ISDB with destination IPs and Ports relevant to that signature. YouTube example:

```
FG # diagnose sys virtual-wan-link internet-service-ctrl-list
Ctrl application(YouTube 31077):Internet Service ID(4294836224)
        Protocol(6), Port(443)
        Address(6): 172.217.28.86 187.181.68.45 172.217.30.33 216.58.202.142
172.217.28.142 209.85.224.201
Ctrl application(YouTube_Video.Play 38569):Internet Service ID(4294836225)
        Protocol(6), Port(443)
        Address(2): 187.181.68.45 209.85.224.201
FG # diagnose sys virtual-wan-link internet-service-ctrl-flush
```

List all IPs/Ports for the dynamic database

Clear the dynamic database (if needed)

FortiOS SD-WAN Rules – Application Control

Rules – Application Control - How it works?

- Enable SSL Deep Inspection to improve application detection
  - » But it's not mandatory
- For Google signatures (like YouTube) you need block QUIC
- Require FortiCare subscription for signature updates
- There is a 32 Server IP limit for this cache (per identified App)

FortiOS SD-WAN Rules

Rules – Hold Time

6.0.1

A hold time parameter and defines the first member link as the primary link, the others as the back-up links. In case, the **primary link downgrade its quality**, the service will switch to the back-up links **without hold**.

In case active back-up links downgrade with lower quality with primary link, this downgraded states should **keep hold-time seconds**, and then switch back to primary link. Otherwise, the backup links keep its active state.

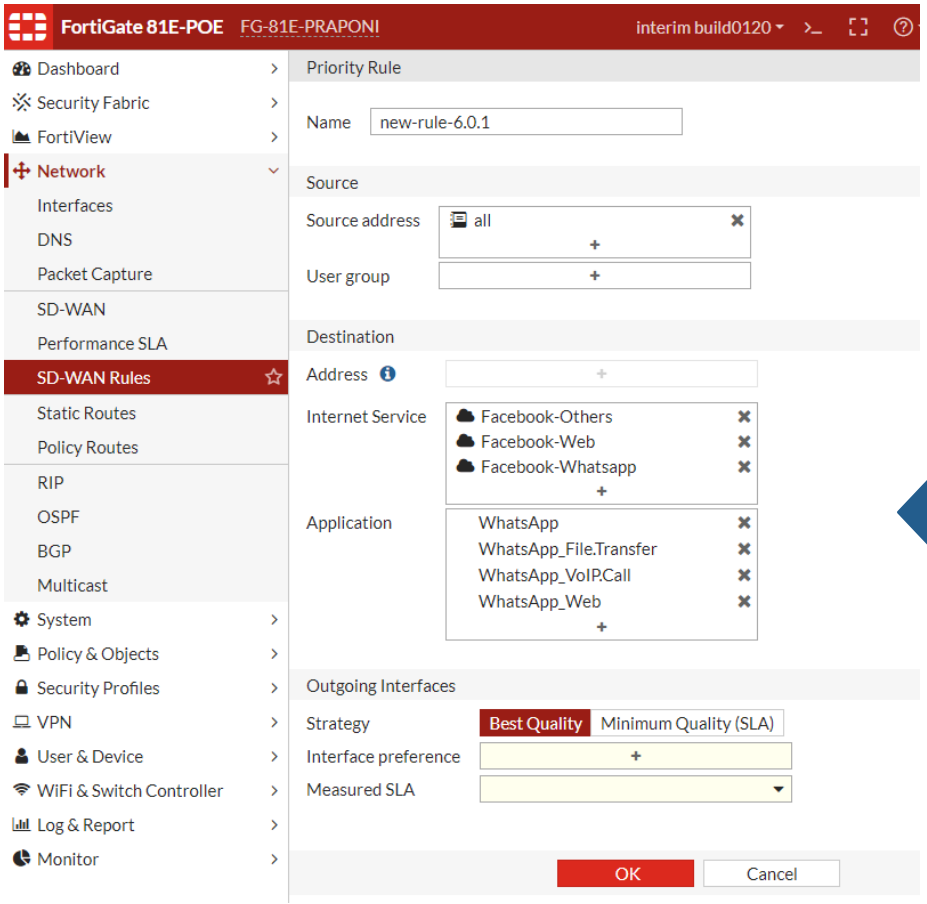
```
config system virtual-wan-link
    config service
      edit 1
        set hold-time 60
    ...
```

Per rule. Default 0

FortiOS SD-WAN Rules

Rules – New Rule interface

6.0.1



In FortiOS 6.0.1, the Rules interface has been changed. Now it's possible to mix **ISDB** and **Application** signatures in the same rule.

It's not possible to select **Address** with others Destinations at the same time

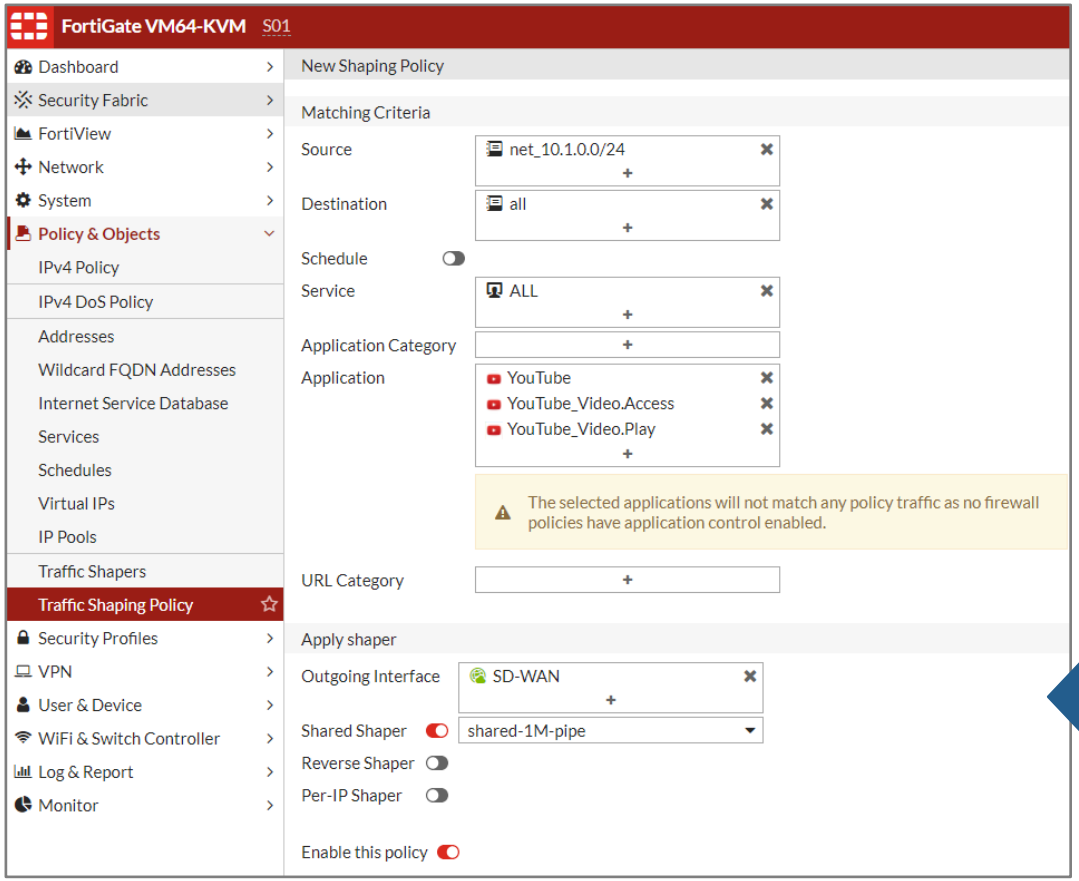
FortiOS SD-WAN

Additional Features

FORTINET

FortiOS SD-WAN

Traffic Shaping



Traffic Shaping

- L7 Analysis for QoS rules based on Users, Apps, URLs…
- Use App Classification to control, bandwidth reservation, limitation, Diffserv marking and prioritization

*SD-WAN interface available as **Traffic Shaping** outgoing interface*

FortiOS SD-WAN

Traffic Shaping - Percentage

This new feature introduces the concept of **shaping-profile** to be attached on a 'system.interface' to shape traffic of an interface. Each shaping-entry of a shaping-profile defines the **Percentage** of the interface bandwidth that can be allocated for one type of classified traffic, as well as priority of that type of traffic; while traffic is classified by shaping-policy entries.

With the presence of **SD-WAN** (virtual-wan-link), shaping-profile entries **make shaping more flexible**. Since SD-WAN can direct traffic to any links, which may have different bandwidth, defining the percentage of interface bandwidth for each classified traffic makes more sense.

- **Until FortiOS 5.6**

Based on traffic-shaper attached to traffic session. Works on L3/L4 and L7

- **New on FortiOS 6.0**

Based on shaping-profile attached to interface. Works on L2

FortiOS SD-WAN

Traffic Shaping – Percentage

```
FG # config firewall shaping-profile
edit "shap1"
  set default-class-id 3
    config shaping-entries
      edit 1
        set class-id 3
        set guaranteed-bandwidth-percentage 10
        set maximum-bandwidth-percentage 10
      next
      edit 2
        set class-id 5
        set guaranteed-bandwidth-percentage 20
        set maximum-bandwidth-percentage 20
        set priority 5
      next
      edit 3
        set class-id 6
        set guaranteed-bandwidth-percentage 40
        set maximum-bandwidth-percentage 40
      next
      end
   next
end
```

Create a **shaping-profile**

default-class-id must be defined for un-classified traffic

Define **class-id** number, **guaranteed-bandwidth-percentage (%)**, **maximum-bandwidth-percentage (%)** and **priority** per class

FortiOS SD-WAN

Traffic Shaping – Percentage

```
FG # config firewall shaping-policy
 edit 1
    set service "ALL"
    set dstint "wan1"
    set class-id 5
    set srcaddr "10.1.100.41"
    set dstaddr "all"
  next
  edit 2
    set service "ALL"
    set dstint "wan1"
    set class-id 6
    set srcaddr "10.1.100.42"
    set dstaddr "all"
  next
end
```

Assign **class-id** to a **shaping-policy**

FortiOS SD-WAN

Traffic Shaping – Percentage

```
FG # config system interface
  edit "wan1"
  ...
    set outbandwidth 1000
    set egress-shaping-profile "shap1"
  ...
  next
end
```

Configure **outbandwidth (kbps)** and apply **shaping-profile** to a interface

FortiOS SD-WAN

Traffic Shaping – Percentage

```
FG # diag netlink interface list wan1

if=wan1 family=00 type=1 index=6 mtu=1500 link=0 master=0
ref=25 state=off start fw_flags=30 flags=up broadcast run allmulti multicast
Qdisc=mq hw_addr=90:6c:ac:fe:cb:91 broadcast_addr=ff:ff:ff:ff:ff:ff
egress traffic control:
         bandwidth=1000(kbps) lock_hit=0 default_class=3 n_active_class=3
            class-id=3    allocated-bandwidth=100(kbps)   guaranteed-bandwidth=100(kbps)
                          max-bandwidth=100(kbps)         current-bandwidth=0(kbps)
                          priority=high   total_bytes=256K        drop_bytes=246
            class-id=5    allocated-bandwidth=200(kbps)   guaranteed-bandwidth=200(kbps)
                          max-bandwidth=200(kbps)         current-bandwidth=0(kbps)
                          priority=high   total_bytes=0           drop_bytes=0
            class-id=6    allocated-bandwidth=400(kbps)   guaranteed-bandwidth=400(kbps)
                          max-bandwidth=400(kbps)         current-bandwidth=0(kbps)
                          priority=high   total_bytes=0           drop_bytes=0
...
```

List the current interface shaping settings

Check the **allocated**, **max**, **guaranteed** and **current** bandwidth per class including the **default class-id**

FortiOS automatically convert bandwidth from % to kbps

FortiOS SD-WAN

Traffic Shaping – Percentage

```
FG # diag sys session list

session info: proto=6 proto_state=01 duration=561011 expire=3172 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class-id=5 shaping-policy_id=1 ha_id=0 policy_dir=0 tunel=/ vlan_cos=0/255
state=may_dirty npu synced syn_ses
statistic(bytes/packets/allow_err): org=837927/8964/1 reply=918808/13348/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
...
```

class-id is identified on session list

FortiOS SD-WAN

Traffic Shaping – Percentage - How it works?

- **guaranteed-bandwidth-percentage** must be no bigger than **maximum-bandwidth-percentage**
- **guaranteed-bandwidth-percentage** of all entries in one profile must be no bigger than 100%
- **guaranteed-bandwidth-percentage** is the bandwidth always reserved for this class
- **maximum-bandwidth-percentage** is the hard limit for the class
- **priority** decides that which class can win when multiple classes are competing for the available bandwidth on the interface
- When same **priority** classes compete for available bandwidth, the allocation to each classes will be proportional to it's guaranteed-bandwidth-percentage
- **default-class-id** must be defined for each *shaping-profile*. The traffic *un-classified* or classified but not defined in shaping-profile, will be treated as default class

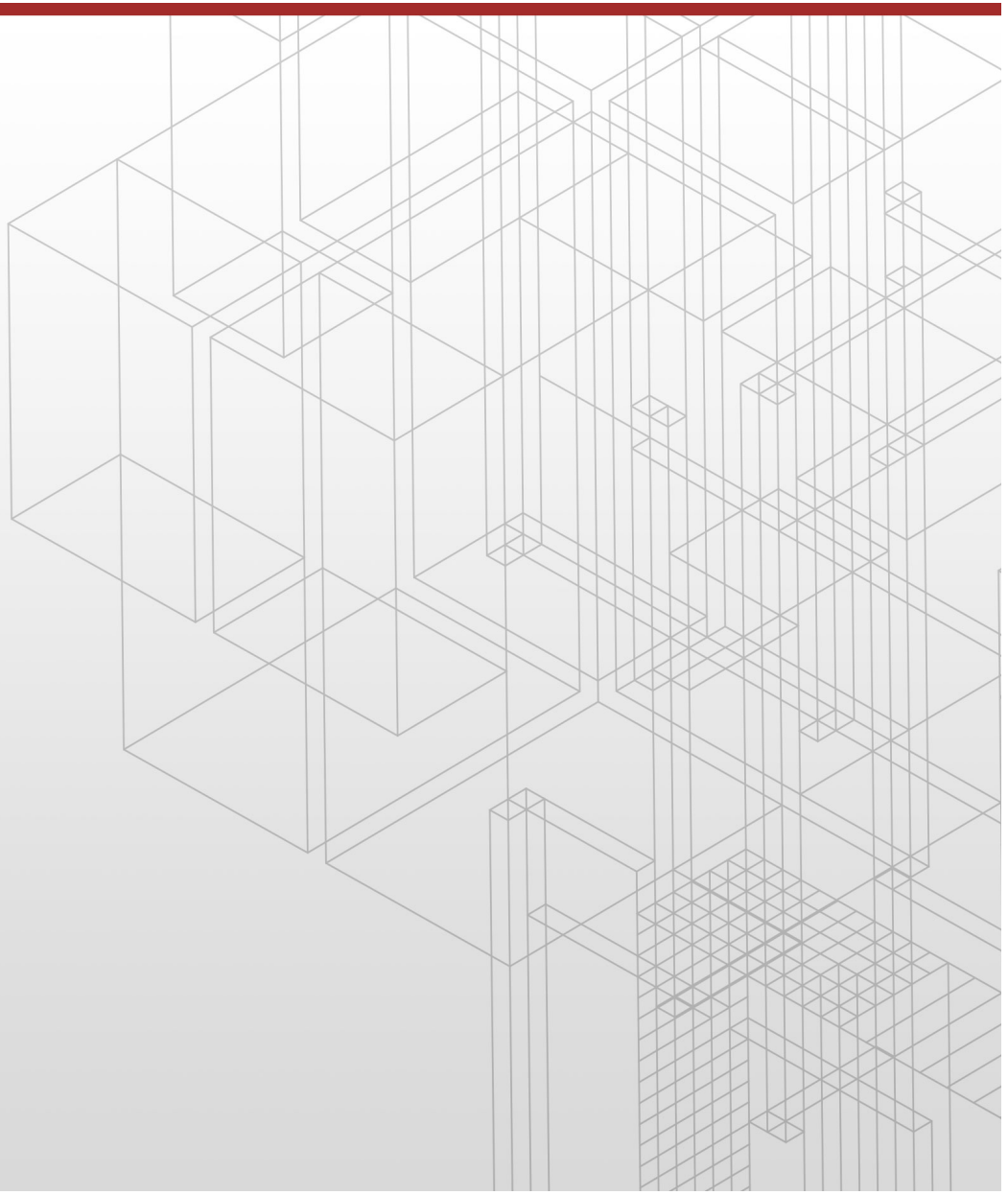
FortiOS SD-WAN

Traffic Shaping – Percentage - Limitations

- CLI only
- Does not support NP offloading
- Does not support SNMP statistics

FortiOS SD-WAN

Zero Touch Provisioning



FortiOS SD-WAN

Zero Touch Provisioning

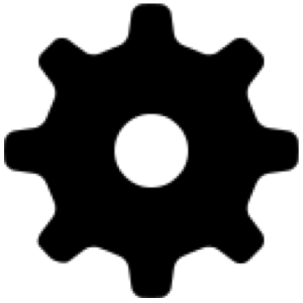
Pre-Provisioning

Model Device

FortiOS SD-WAN

Zero Touch Provisioning

Automated Provisioning



API

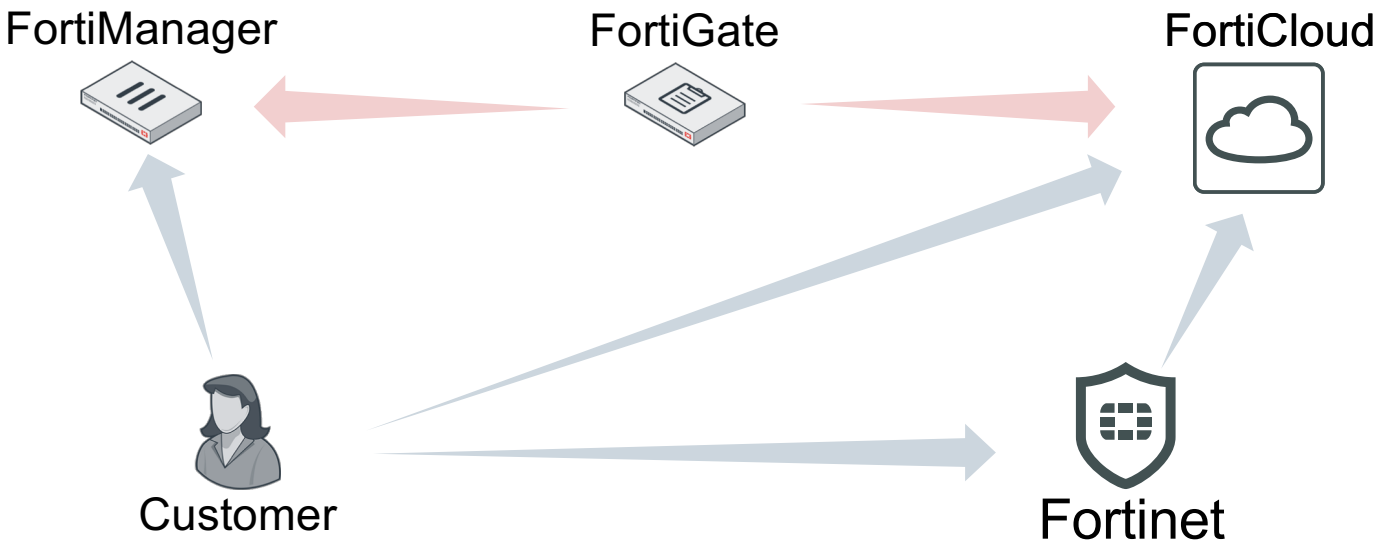
Zero Touch Provisioning

FortiDeploy

FortiOS SD-WAN

Zero Touch Provisioning – How it works ?

Deployed device will fetch its *management* details from FortiCloud



FortiOS SD-WAN

Zero Touch Provisioning – Step-by-Step

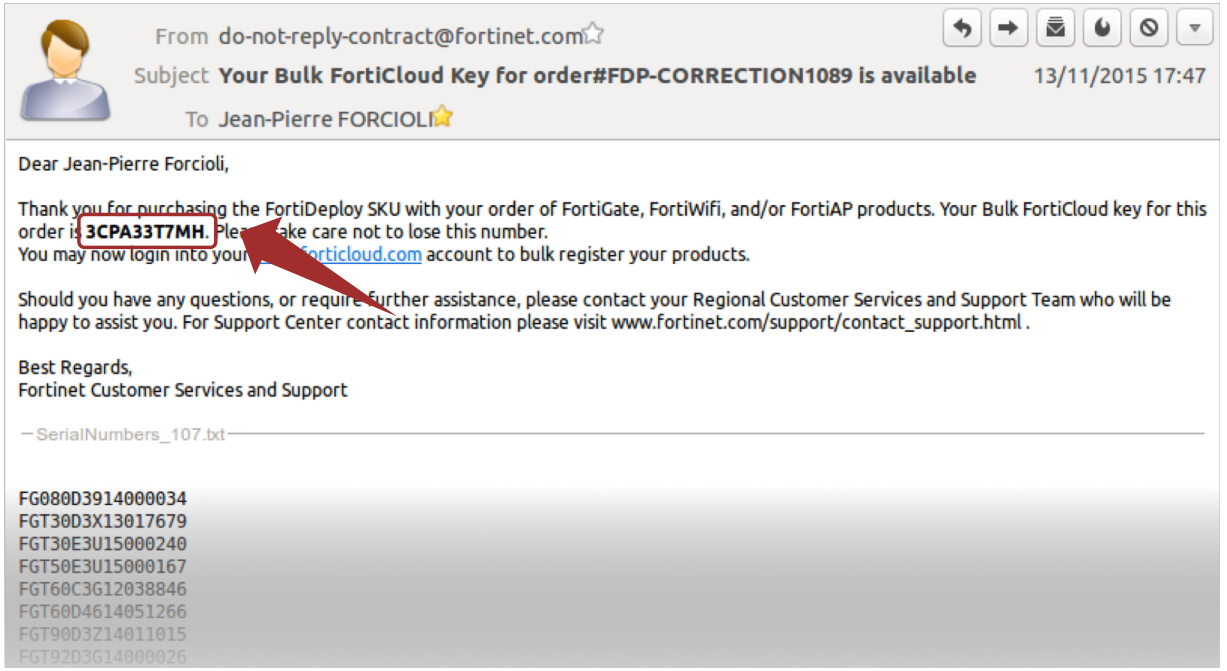
Order the FortiGates along with a FortiDeploy SKU

Model	SKU	Description	Quantity
FortiGate-30D	FG-30D	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports). Max managed FortiAPs (Total / Tunnel) 2 / 2	1
FortiGate-30E	FG-30E	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports). Max managed FortiAPs (Total / Tunnel) 2 / 2	1
FortiGate-50E	FG-50E	25 x GE RJ45 Ports (including 1 x Management port, 20 x PoE ports, 4 x PoE+ ports). Max managed FortiAPs (Total / Tunnel) 10 / 5	1
FortiGate-60C	FG-60C	25 x GE RJ45 Ports (including 1 x Management port, 20 x PoE ports, 4 x PoE+ ports). Max managed FortiAPs (Total / Tunnel) 10 / 5	1
FortiGate-60D	FG-60D	10 x GE RJ45 ports (including 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port). Max managed FortiAPs (Total / Tunnel) 10 / 5	1
FortiGate-80D	FG-80D	4x GE RJ45 ports, 16GB onboard storage, Max managed FortiAPs (Total / Tunnel) 32 / 16	1
FortiGate-90D	FG-90D	16 x GE RJ45 ports (2x WAN ports, 14x Switch ports), 32GB onboard storage. Max managed FortiAPs (Total / Tunnel) 32 / 16	1
FortiGate-92D	FG-92D	16 x GE RJ45 ports (2x WAN ports, 14x Switch ports), 16GB onboard storage. Max managed FortiAPs (Total / Tunnel) 32 / 16	1
FortiDeploy	FDP-SINGLE-USE	Enables zero touch bulk provisioning for your FortiGate, FortiWifi, or FortiAP products.	1

FortiOS SD-WAN

Zero Touch Provisioning – Step-by-Step

Fortinet registers your devices in FortiCloud



From do-not-reply-contract@fortinet.com

Subject **Your Bulk FortiCloud Key for order#FDP-CORRECTION1089 is available** 13/11/2015 17:47

To Jean-Pierre FORCIOLI

Dear Jean-Pierre Forcioli,

Thank you for purchasing the FortiDeploy SKU with your order of FortiGate, FortiWifi, and/or FortiAP products. Your Bulk FortiCloud key for this order is **3CPA33T7MH**. Please take care not to lose this number.
You may now login into your forticloud.com account to bulk register your products.

Should you have any questions, or require further assistance, please contact your Regional Customer Services and Support Team who will be happy to assist you. For Support Center contact information please visit www.fortinet.com/support/contact_support.html .

Best Regards,
Fortinet Customer Services and Support

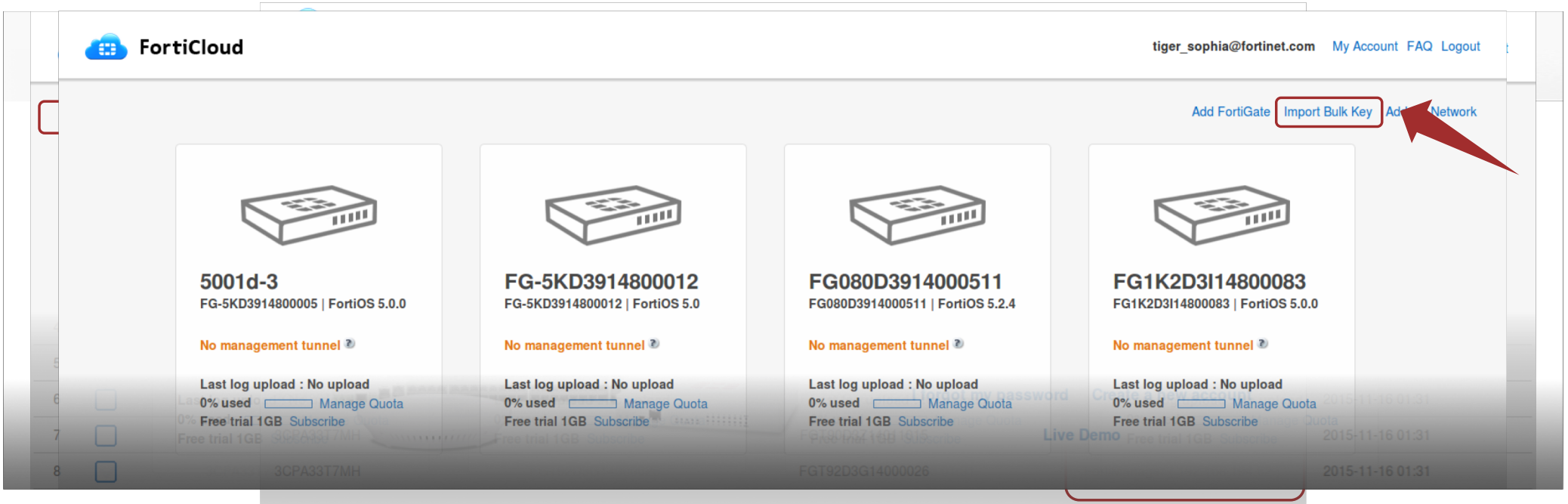
SerialNumbers_107.txt

FG080D3914000034
FGT30D3X13017679
FGT30E3U15000240
FGT50E3U15000167
FGT60C3G12038846
FGT60D4614051266
FGT90D3Z14011015
FGT92D3G14000026

FortiOS SD-WAN

Zero Touch Provisioning – Step-by-Step

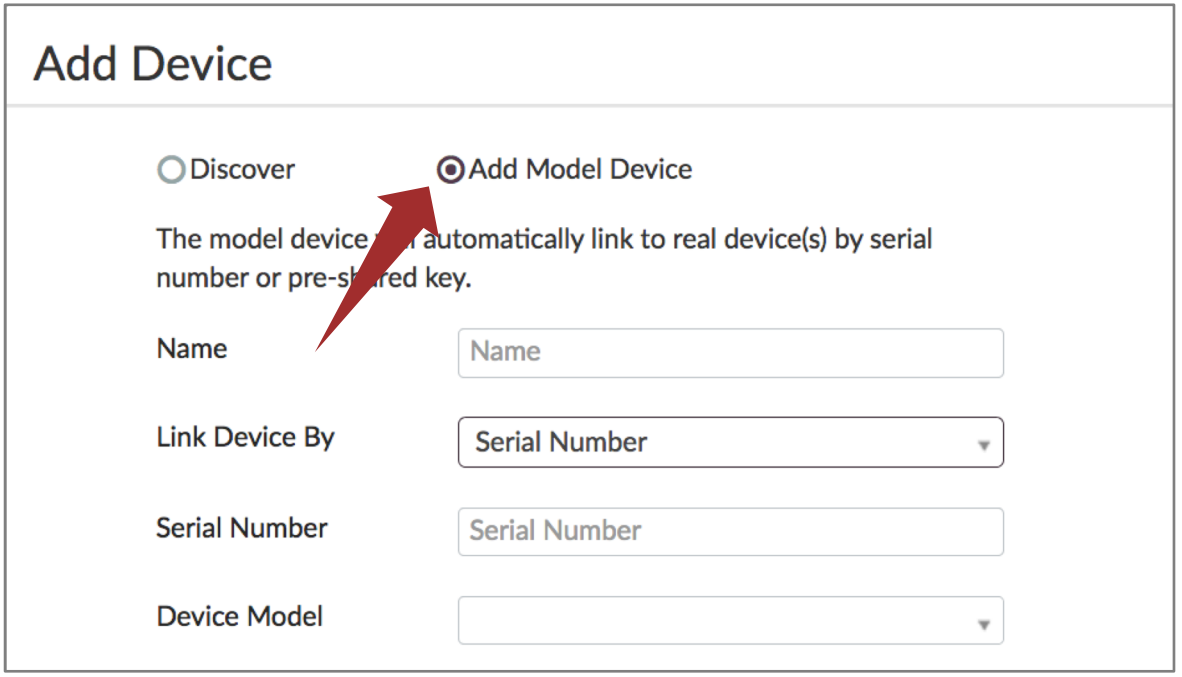
Assign FortiManager IP to registered devices



FortiOS SD-WAN

Zero Touch Provisioning – Step-by-Step

Add Device Wizard



FortiOS SD-WAN

Zero Touch Provisioning – Step-by-Step

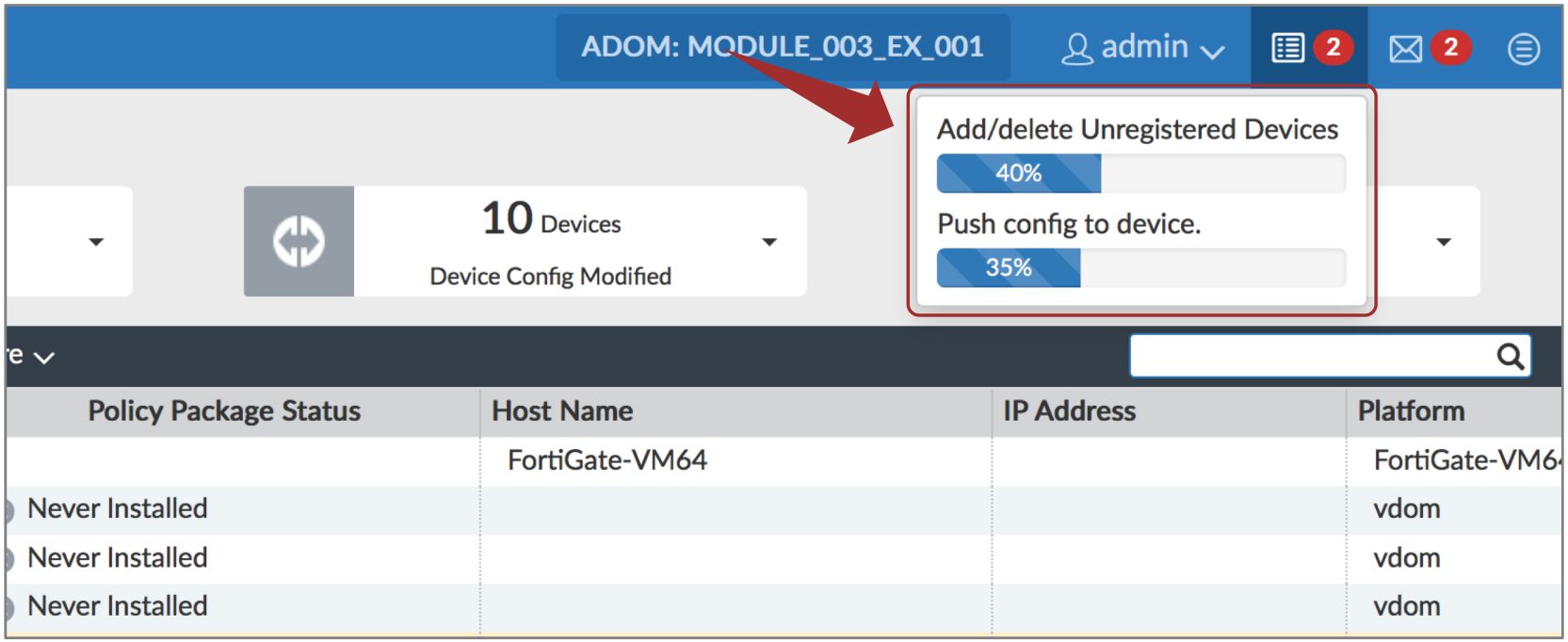
Deployed device will fetch its management details from FortiCloud

```
FG # diagnose debug cli 8
FG # diagnose debug enable
[...]
0: config system fortiguard
0: set service-account-id "tiger_sophia@fortinet.com"
0: end
[...]
0: config system central-management
0: set type fortimanager
0: set fmg 192.168.194.62
0: set mode normal
```

FortiOS SD-WAN

Zero Touch Provisioning – Step-by-Step

FMG will auto-push the provisioned configuration



FortiOS SD-WAN

Zero Touch Provisioning - FMG API

Automate the Mass Device Deployment process

FMG API

FortiDeploy

Add Model Device

Provision Model Device

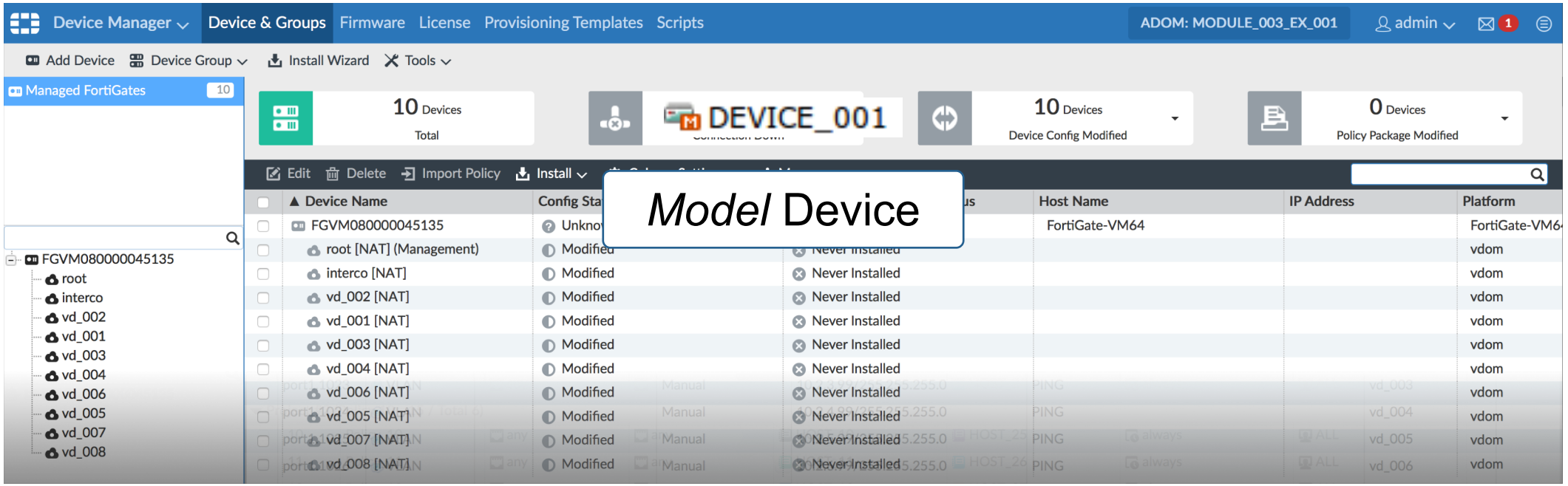
Promote Model Device

Deploy Real Device

FortiOS SD-WAN

Zero Touch Provisioning – FMG API

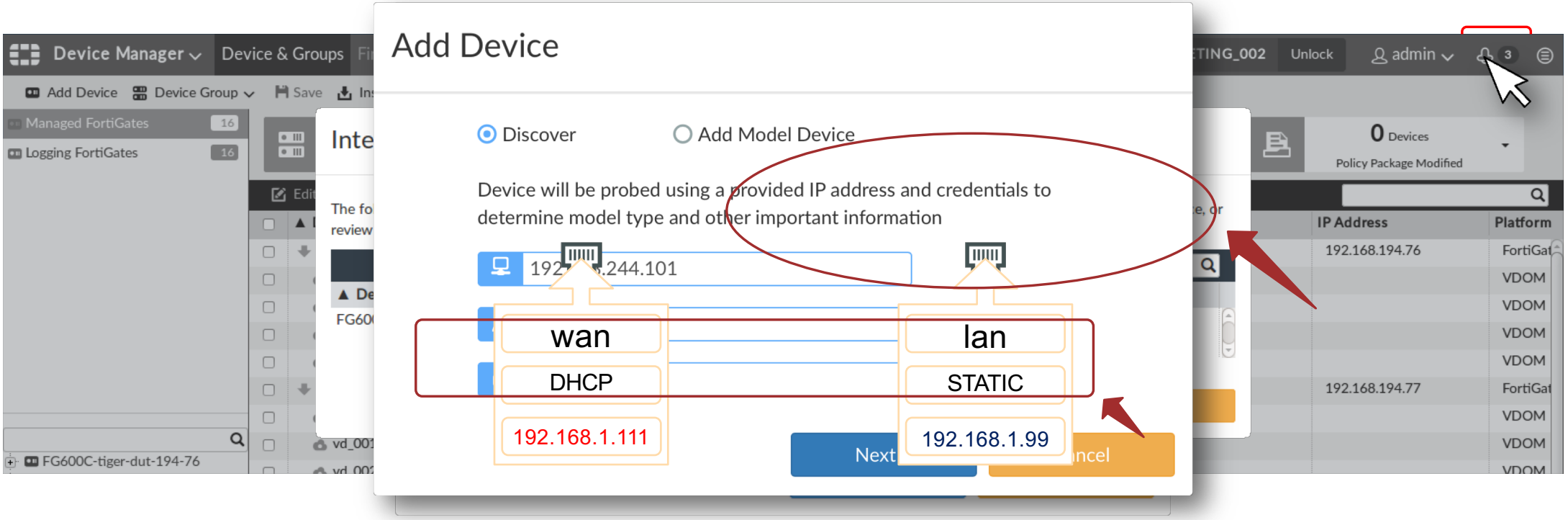
Provision your devices in FortiManager



FortiOS SD-WAN

Zero Touch Provisioning – FortiDeploy Conflicting IPs Detection

FortiDeploy supported models may encounter IP conflict



FortiManager SD-WAN

FORTINET

FortiManager SD-WAN

Feature Support

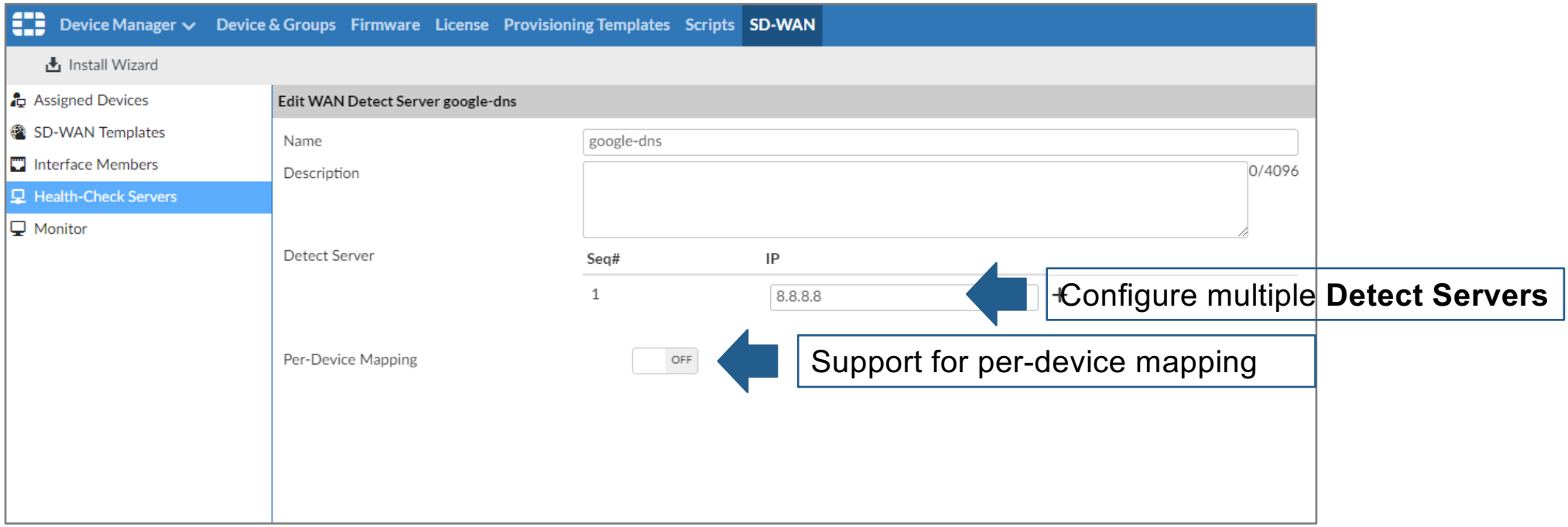
- SD-WAN Central Template
  - » You can centrally provision SD-WAN templates by specifying SD-WAN interface members, WAN link performance criteria, and application routing priority
- SD-WAN Monitoring
  - » Map View displays SD-WAN enabled devices on Google Map with color coded icons. Mouse over to view health performance statistics for each SD-WAN link member
  - » Table View provides more granular information on each SD-WAN link member such as link status, applications performance and their bandwidth usage

FMG is not able to import SD-WAN configuration from FortiGate. You need to create a new SD-WAN template to use all central management features like unified profile.

FortiManager SD-WAN

SD-WAN Central Template – Health-Check

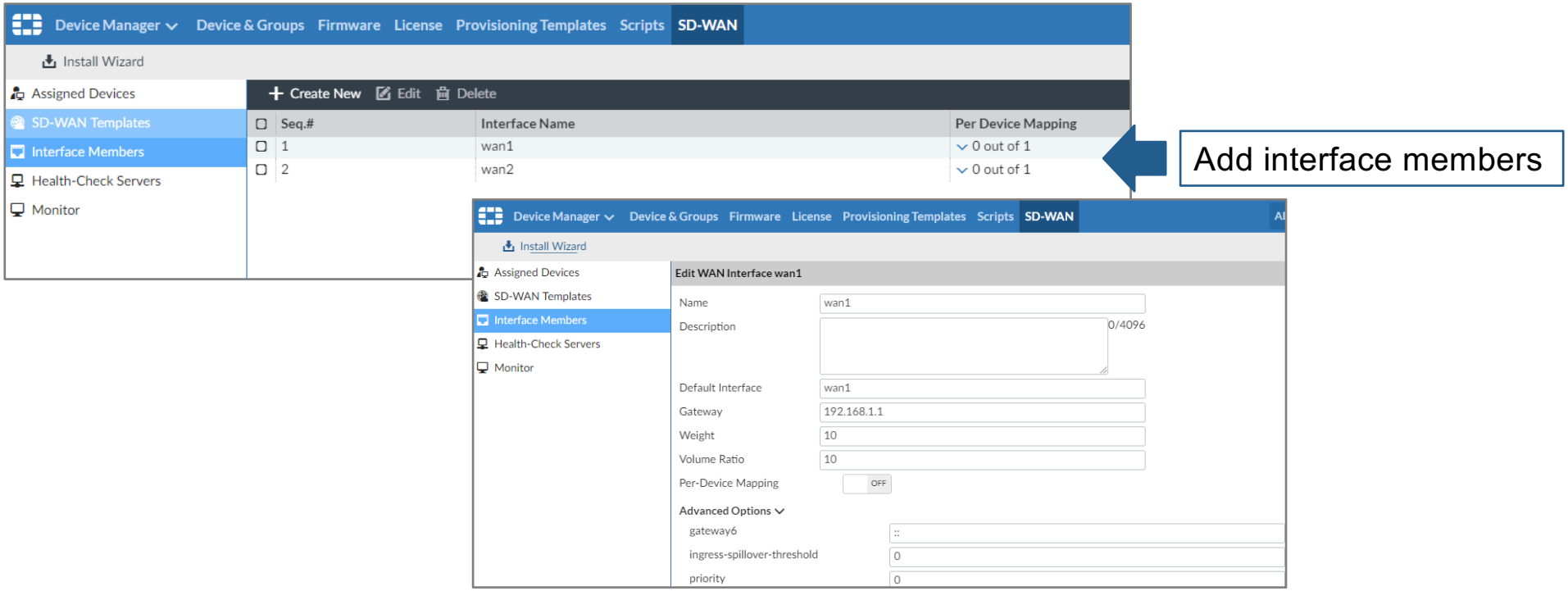
- Create Health-Check Servers



FortiManager SD-WAN

SD-WAN Central Template – Interface

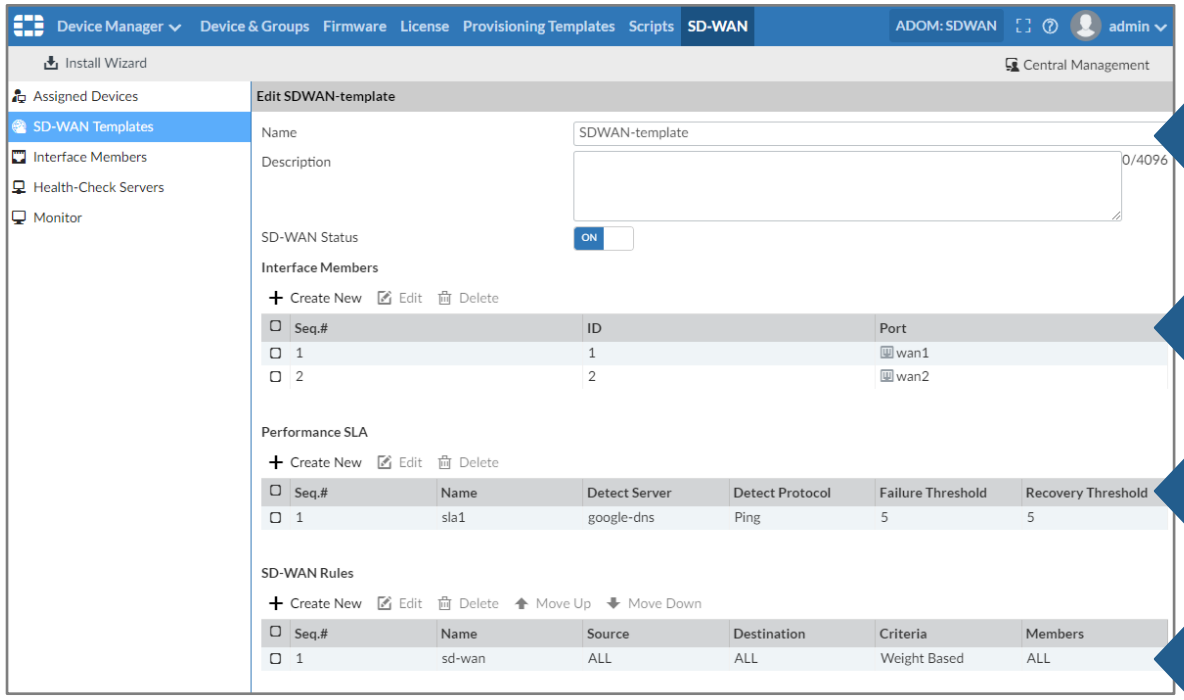
- Add Interface Members



FortiManager SD-WAN

SD-WAN Central Template – Put it all together

- Create SD-WAN Template



Create a new template

Add interfaces

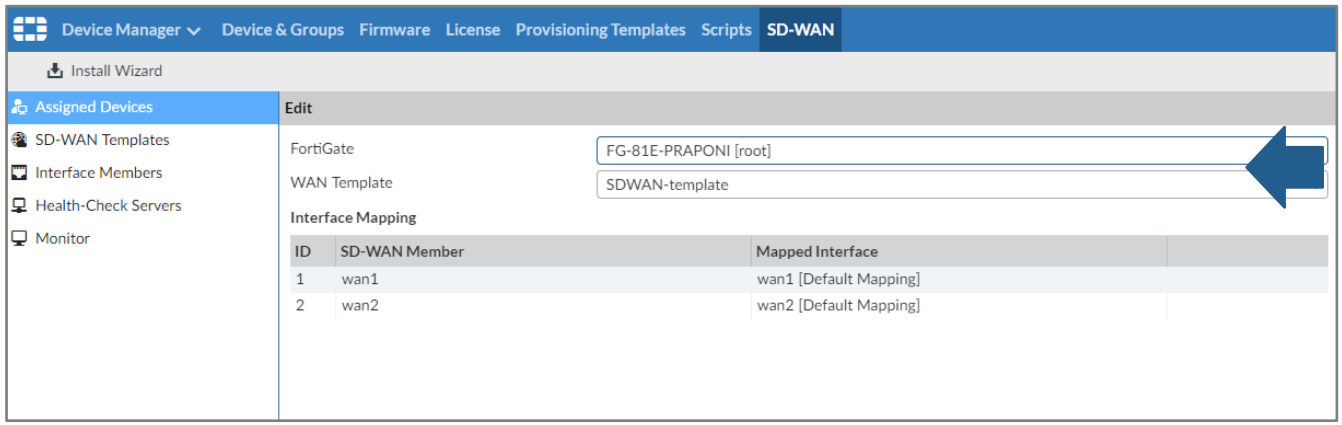
Create a Performance SLA with targets and add the Health-Checks

Configure SD-WAN Rules

FortiManager SD-WAN

SD-WAN Central Template – Assigned Devices

- Assign to devices

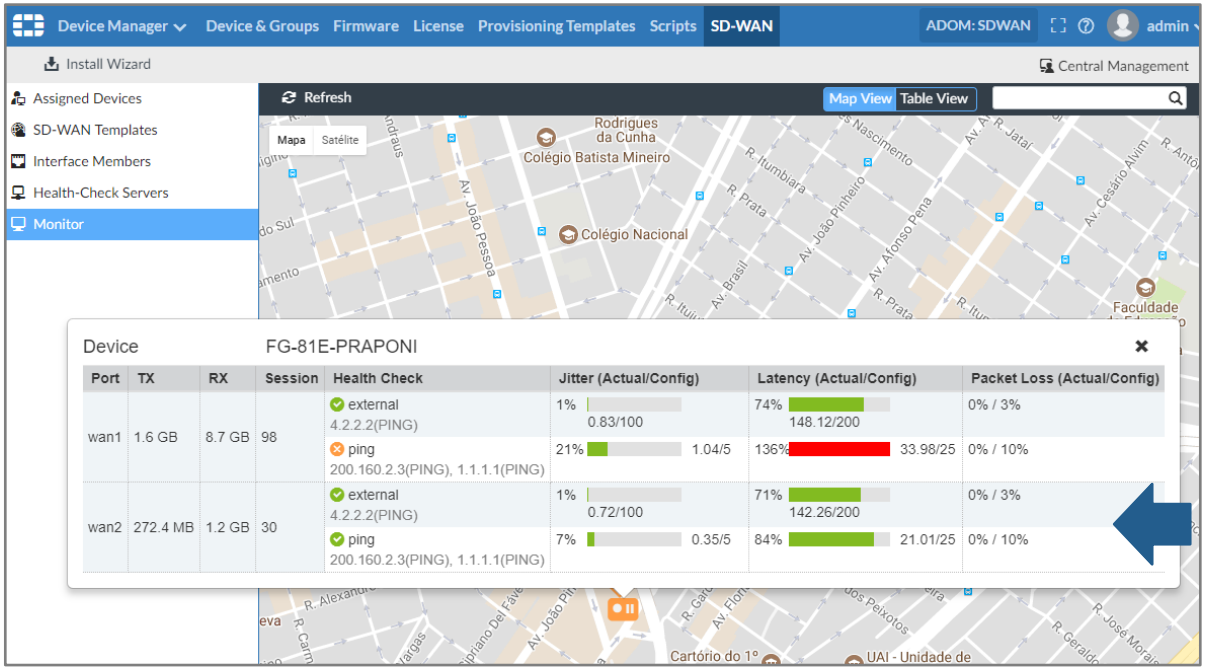


Assigned devices and template to SD-WAN

- Deploy with **Install Wizard**

FortiManager SD-WAN

SD-WAN Monitor



SD-WAN Monitors are imported from FortiGate, so it will work even without SD-WAN Template

In the Google Maps you can select the device and it shows all Health-Checks

Monitor show the actual status of the Health-Checks. If the value is above SLA target, this is marked as red in the graph

FortiManager SD-WAN

SD-WAN Monitor

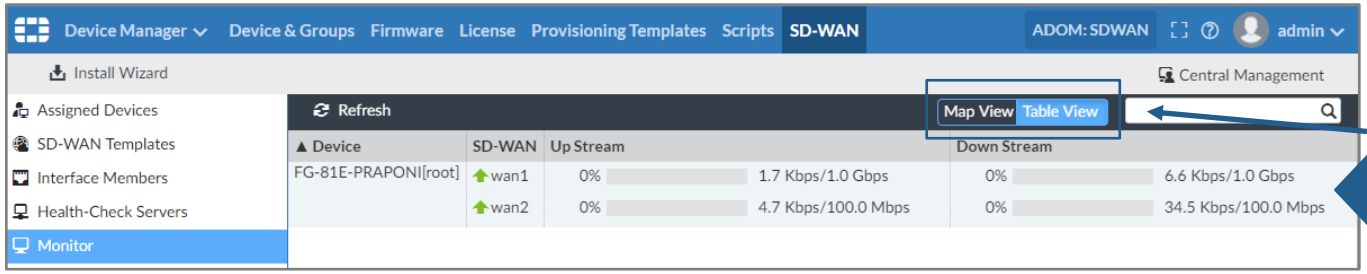


Table View with Up Stream and Down Stream usage

The first row in Table View shows data from the first FortiGate device that connects to FortiManager. Only the first five Internet Services for the first FortiGate device are shown in Table View. The Internet Services for the other FortiGate devices in the table are shown only if they contain one or more of the first five Internet Services shown by the first FortiGate device

Quiz

Day 02 Recap

FortiOS SD-WAN

Additional Features

FORTINET

FortiOS SD-WAN

Dynamic Routing – Route Tag

```
config router router-map
    edit "comm1"
      config rule
        edit 1
          set match-community "30:5"
          set set-route-tag 15
        next
      ...
```

```
config system virtual-wan-link
    ...
    config service
      edit 1
        set mode priority
        set router-tag 15
        set health-check "ping"
        set link-cost-factor jitter
        set priority-members 1 2
      next
    ...
```

BGP Support Added
CLI configuration only
BGP router-map and community

FortiOS SD-WAN

Dynamic Routing – Route Tag

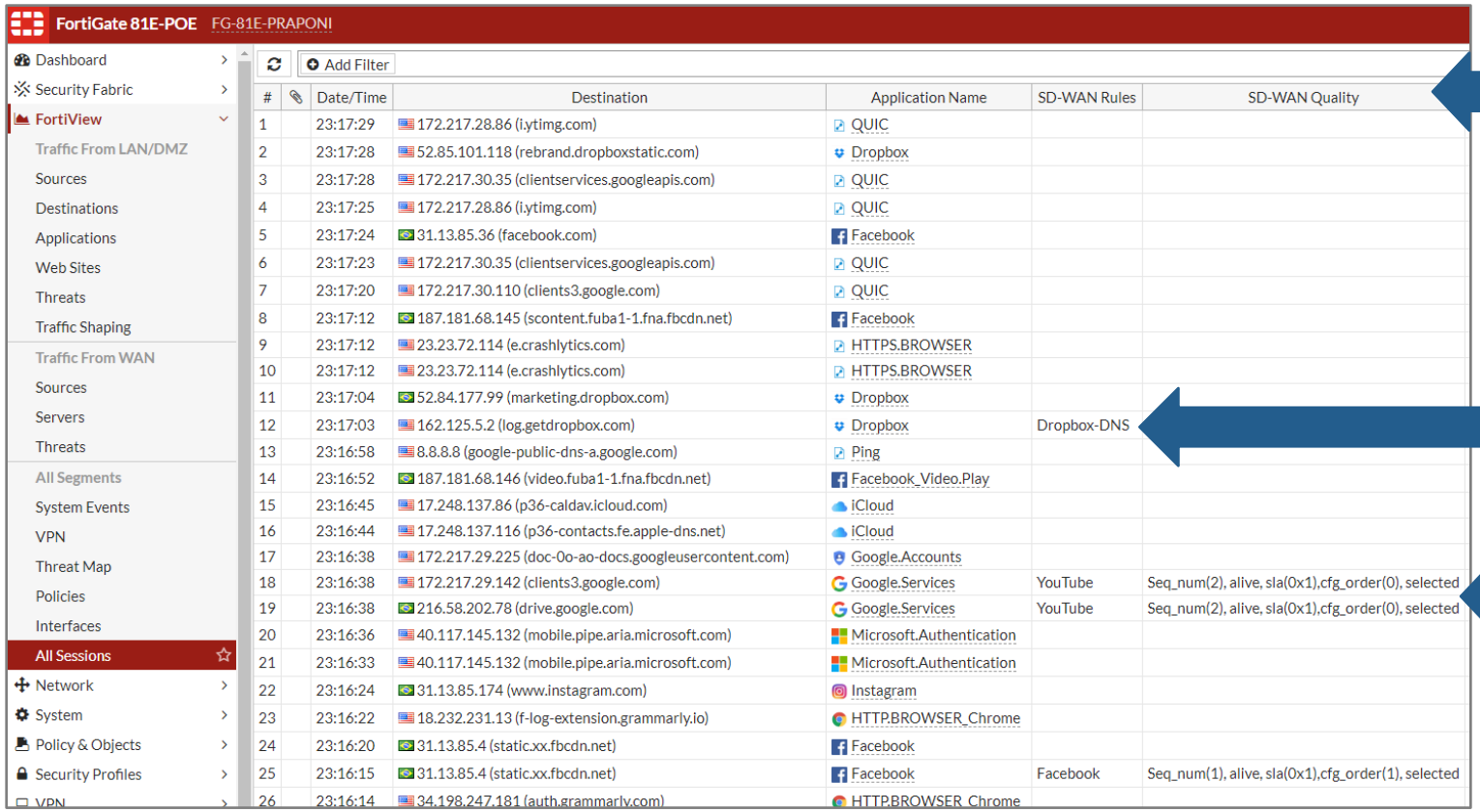
```
FG # get router info bgp network 10.100.10.0
BGP routing table entry for 10.100.10.0/24
Paths: (2 available, best #1, table Default-IP-Routing-Table)
...
  10.100.1.5 from 10.100.1.5 (6.6.6.6)
    Origin EGP metric 200, localpref 100, weight 10000, valid, external, best
    Community: 30:5
...

FG # get router info route-map-address
Extend-tag: 15, interface(port15:16)
        10.100.10.0/255.255.255.0

FG # diag sys virtual-wan-link service
Service(1): flags=0x0
  TOS(0x0/0x0), protocol(0: 1->65535), Mode(priority), …
  Members:
   1: Seq_num(1), alive, jitter: 0.400, selected
   2: Seq_num(1), alive, jitter: 0.400, selected
 Route tag address: 10.100.10.0/255.255.255.0
```

FortiOS SD-WAN

FortiView – All Sessions



Right click and select FortiView SD-WAN columns
Only available with 5 minutes or more

SD-WAN Rule matched by name

SD-WAN SLA Link selection


FORTINET®